"TÜRK CEZA ADALET SİSTEMİNİN ETKİNLİĞİNİN GELİŞTİRİLMESİ"

Avrupa Birliği - Avrupa Konseyi
Ortak Projesi

BİLİŞİM SUÇLARI, SORUŞTURMA VE KOVUŞTURMA YÖNTEMLERİ İLE İNTERNET VE İLETİŞİM HUKUKU UYGULAMA REHBERİ

• • •

Hazırlayanlar

• • •

Yrd. Doç. Dr. Murat Volkan Dülger
(Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet ve İletişim Hukuku)

• • •

Av.Gözde Modoğlu
(Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet ve İletişim Hukuku)

Bu kitap "Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi" başlıklı, Avrupa Birliği/ Avrupa Konseyi/ Türkiye Cumhuriyeti Devleti tarafından finanse edilen ve Avrupa Konseyi tarafından yürütülen Avrupa Birliği/ Avrupa Konseyi Ortak Projesi kapsamında basılmıştır.T.C. Adalet Bakanlığı, Hâkimler ve Savcılar Yüksek Kurulu, Türkiye Adalet Akademisi ve Türkiye Barolar Birliği bu projenin yararlanıcısıdır. Projenin ihale makamı Merkezi Finans ve İhale Birimi'dir.

1 BİLİŞİME İLİŞKİN DÜZENLEMELER

BİLİŞİM SUÇLARINDA SORUŞTURMA TEKNİKLERİ VE DELİL ELDE ETME YÖNTEMLERİ UYGULAMA REHBERİ

1. BİLİŞİME İLİŞKİN DÜZENLEMELER

Bilişim suçu kavramı esas olarak TCK'nın 10. bölümünde yer alan 243-246. maddeleri arasında düzenlenmektedir. Anılan maddeler yakından incelendiğinde kanunkoyucunun bu hükümlerde bilişim sistemlerine hariçten yapılan müdahaleleri (sisteme izinsiz olarak girme, buradaki verileri değiştirme ya da yok etme, sistemin işleyişini engelleme veya bozma vs.) düzenleme konusu yaptığı görülmektedir.
Bilişim suçları yalnızca TCK'nın 10. bölümünde yer almamaktadır. Bu maddeler dışında bilişim suçu kavramı, bilişim sistemleri kullanılarak gerçekleştirilen tüm suçları da (Örneğin; bilgisayar sistemleri kullanılarak kişinin işlemediğini bildiği bir suç hakkında yetkili makamlara ihbar ve şikâyette bulunmak suretiyle iftira, yine aynı sistemler kullanılarak kişiye hakaret, kişiler arasındaki haberleşmenin gizliliğini bilişim sistemleri kullanılarak ihlal, çocukların cinsel istismarına ilişkin görüntüleri bilgisayarlarda depolamak-yaymak, TCK'nın 142/2-e maddesinde belirtilen nitelikli hırsızlık ve 158/1-f maddesinde belirtilen nitelikli dolandırıcılık fiillerini de) ifade etmektedir. Zîra ilgili suçun gerçekleşip gerçekleşmediğinin tespitinde TCK'nın 243-246. maddelerinde yer alan bilişim suçlarının soruşturulmasında uygulanan soruşturma usulleri (Örneğin, suça konu ileti veya fiilin hangi IP numaralı bilgisayardan gönderildiği veya yapıldığının tespiti, daha sonra belirlenen IP numaralı bilgisayarın sahibi olan şüphelinin bilgisayarından imaj alma, daha sonra bu verilerin bilirkişiler vasıtasıyla incelenmesi gibi) tatbik edilecektir. Sonuçta bilişim sistemi kullanılarak işlenen suç (örneğin sosyal paylaşım sitelerinde müştekiye edilen hakaret gibi) aslî hüviyetini (yani hakaret suçunu) muhafaza etmekteyse de bu durum onun bilişim sistemi kullanılarak işlendiği gerçeğini etkilememektedir. Bunun dışında TCK'nın 243-245.maddelerinde belirtilen bilişim suçlarının soruşturulması sırasında yaşanan sorunların (kolluk ve Adlî personelin bu suçlar ile ilgili yeterli bilgiye ve tecrübeye sahip olmamaları gibi) aynısı, bilişim sistemleri kullanılarak gerçekleştirilen diğer suçların soruşturulması sırasında da yaşanmaktadır.

Bu gerekçelerle çalışmamızda TCK'nın 243-246.maddeleri arasında düzenlenen bilişim suçları ile birlikte bu maddeler arasında sayılmayan ancak bilişim sistemleri kullanılarak işlenmesi mümkün olan diğer suç tipleri de inceleme konusu yapılmıştır. Aslında pek çok klasik suçun da bilişim sistemleri aracılığıyla işlenmesi mümkündür. Örneğin; kasten öldürme suçuna azmettiren kişinin aslî faile internet yoluyla maktulü öldürme emrini vermesi, bilgisayar sistemleri kullanarak terör örgütünün propagandasının yapılması gibi. Bu durumlarda da tıpkı bilişim suçlarında olduğu gibi delil araştırması yapılacaktır.

Şimdi yürürlükteki mevzuatta belirtilen bilişim suçları ve bilişim sistemleri kullanılarak işlenebilecek suçların toplu şekilde incelenmesine geçebiliriz:

1.1. Uluslararası Sözleşmeler

1.1.1. Siber Suçlar Sözleşmesi

Siber Suçlar Sözleşmesi'nde, bilişim sistemi olarak bilgisayar sistemlerinin ceza hukukuna etkisi ve ortaya çıkardığı sorunlar, hem maddî ceza hukuku açısından hem de ceza yargılaması açısından ele alınmış ve bu alanlarda bilgisayar sistemlerinin

ASSS, 6533 sayılı Kanun ile kabul edilerek 2 Mayıs 2014 tarihinde Resmî Gazete'de yayınlanarak yürürlüğe girmiştir.

kullanılması merkezinde ortaya çıkan sorunlara ilişkin çözümler getirilmek istenmiştir. Sözleşmenin ikinci kısmını oluşturan maddî ceza hukukuna ve ceza yargılamasına ilişkin sorunlar iki ana bölüme ayrılmıştır. Birinci bölümde, maddî ceza hukukuna ilişkin düzenlemelere yer verilmiştir; ikinci bölümde ise, ceza yargılamasına ilişkin sorunlar ele alınarak özellikle delillerin elde edilmesi, korunması ve saklanmasına ilişkin olarak ortaya çıkan sorunlara çözüm getirilmek istenmiştir.

Siber Suçlar Sözleşmesi'nin 4. başlığıolan "Saklanan bilgisayar verilerinin aranması ve bunlara el koyulması" şu şekilde düzenlenmiştir:

"Madde 19 - Saklanan Bilgisayar Verilerinin Aranması ve Bunlara El Konulması

1. Taraflardan her biri, yetkili mercilerinin kendi ulusal sınırları içinde aşağıdakileri arama ya da bunlara benzer şekilde erişim sağlama konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

a. Bir bilgisayar sistemi ya da bu sistemin parçası ve bunlarda saklanan bilgisayar verileri,
b. Bilgisayar verilerinin saklandığı cihazları.

2. Tarafların her biri, yetkili mercilerinin paragraf 1 (a) uyarınca belirli bir bilgisayar sisteminde ya da bu sistemin bir parçasında arama yapması ya da bunlara erişim sağlaması söz konusu olduğunda, ayrıca aranan verilerin kendi ulusal sınırları içindeki başka bir bilgisayar sisteminde ya da bu sistemin bir parçasında saklandığına dair gerekçeleri bulunduğunda, söz konusu mercilerin arama ya da erişim işlemlerini bu sistemi kapsayacak şekilde genişletebilmelerini sağlamak üzere gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

3. Taraflardan her biri, yetkili mercilerinin kendi ulusal sınırları içinde paragraf 1 veya 2 uyarınca erişilen bilgisayar verilerine el koyma ya da bunları başka şekillerde koruma altına alınması konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Bu işlemler arasında, aşağıdakilerin yapılabilmesine yönelik yetkilerin sağlanması bulunacaktır:

a. Herhangi bir bilgisayar sistemine ya da bu sistemin bir parçasına veya bilgisayar verilerinin saklandığı cihazlara el konulması ya da bunların benzer şekilde koruma altına alınması,
b. Bu bilgisayar verilerinin kopyalanıp alıkonulması,
c. Söz konusu saklı bilgisayar verilerinin doğruluğunun muhafaza edilmesi,
d. Erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez kullanılamaz hale getirilmesi ya da silinmesi.

4. Taraflardan her biri, yetkili mercilerinin ilgili bilgisayar sisteminin işleyişi hakkında ya da bu sistem içindeki bilgisayar verilerinin korunması için kullanılan önlemler hakkında bilgi sahibi olan herhangi bir kişiye, paragraf 1 ve 2'de belirtilen işlemlerin yapılabilmesi için gerekli bilgileri makul şekilde vermesi yönünde talimat vermesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

5. İşbu maddede sözü geçen yetki ve usuller madde 14 ve 15'e tabi olacaktır."

Sözleşmeye taraf olan ülkelerin, bu normları kendi iç hukuklarına uyarlaması

gerekmekte olup sözleşmede bu hususta sıkça bahsedilmiştir.

Maddenin birinci fıkrasında yetkili mercilerin arama ya da erişim sağlama konusunda yetkili olabilmeleri için "bilgisayar sistemi, bilgisayar parçası ve bunlarda saklanan bilgisayar verileri" cümlesi ile yetinilmemiş olup "bilgisayar verilerinin saklandığı cihazları" ifadesine yer verilmiş ve böylece CMK'da bahsetmiş olduğumuz eksiklik giderilmiştir. Bilgisayar belirli komutlara göre veri işleyen ve depolayan bir makine olduğundan, tüm fiziksel parçaları kapsam dâhilindedir. Sözleşmenin birinci maddesi daha genel bir tanım öngörerek makineye ait tüm fiziksel donanımı değil, bilgisayar verilerinin saklandığı cihazlardan bahsetmiştir. Bu şekilde uygulamada kolaylık yaratılarak, tüm bilgisayarı külliyen aramak ve koşulları oluştuğunda elkoymak yerine, yalnızca HDD veyahut DVD'lere aynı işlem uygulanabilecektir. Maddenin ikinci fıkrası da bilgisayar sisteminin bağlı olduğu diğer sistemleri de kapsayarak somut anlamı genişletmiştir.

Maddenin üçüncü fıkrası, söz konusu bilgisayar verilerine elkonulması, bu verilerin koruma altına alınması ve saklanmasını düzenlemiştir.

Maddenin dördüncü fıkrasında "Adlî bilişim uzmanı" devreye girmiştir. Madde metninde, uzman kişiye, birinci ve ikinci fıkradaki işlemlerin yapılabilmesi için gerekli bilgileri makul şekilde vermesi yönünde talimat verilmesi için gerekli yasal düzenlemenin yapılmasının gerekliliği belirtilmiştir. Ülkemizde bu husus kolluk kuvvetleri tarafından uygulanmakta olup yeterli sayıda Adlî bilişim uzmanı bulunmamaktadır.

Maddenin son fıkrasında ise yetki ve usullerin aynı sözleşmenin 14. ve 15. maddelerine tabi olacağı belirtilmiştir.

1.2. Kanun Hükümleri

1.2.1. Türk Ceza Kanunu:

a. TCK'nın 6/g maddesinde *"Basın ve yayın yolu ile deyiminden; her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar"* suretiyle basın ve yayın yolu ile deyiminden "elektronik kitle iletişim aracıyla yapılan yayınların da anlaşılacağı vurgulanmıştır.

b. TCK'nın 125/2.maddesinde hakaret fiilinin, mağduru muhatap alan sesli, yazılı veya görüntülü bir ileti ile işlenmesi hali de suç sayılmıştır. Örneğin, internet yoluyla gönderilen mesajlar veya sosyal paylaşım sitelerinde karşı tarafa yönelik hakaret içerikli yazı ve mesajlar bu kapsamda değerlendirilebilecektir.

c. TCK'nın 132.maddesinde Haberleşme gizliliğinin ihlali suç sayılmıştır. Buna göre kişiler arasındaki haberleşme gizliliğini ihlal etme, bu haberleşmeyi kayda alma, bunları ifşa etme fiilleri maddeye göre cezalandırılmaktadır. Bunun dışında TCK'nın 6/1-g maddesindeki tanımdan ve yukarıda bu tanıma ilişkin yapılan açıklamadan yola çıkılarak bu gizliliğin ihlali sonucunda elde edilen verilerin basın ve yayın yoluyla (örneğin sosyal paylaşım sitelerinde veya haber sitelerinde) ifşa edilmesi de cezalandırılmayı gerektirmektedir.

d. **TCK'nın 133.maddesinde** kişiler arasındaki aleni olmayan konuşmaların taraflarından birisinin rızası olmaksızın bir alet yardımıyla dinlenilmesi veya ses kayıt cihazı ile kaydedilmesi, aleni olmayan bir söyleşinin diğer konuşanların rızası olmadan kaydedilmesi, 1.fıkrada tanımlanan eylem neticesinde elde edilen verilerin ifşa edilmesi, bu ifşa etmenin TCK'nın 6/1-g maddesinde ve yukarıda belirtilen açıklamalar ışığında basın ve yayın yoluyla yapılması suç olarak tanımlanmıştır. Buna göre örneğin iki kişi arasındaki bir konuşmanın taraflardan birisinin rızası olmadan dinlenilmesi ve daha sonra da internet sitelerinde ifşa edilmesi bu maddenin kapsamına girmektedir.

e. **TCK'nın 134.maddesinde** kişilerin özel hayatının gizliliğini ihlal etmek, bu gizliliği görüntü veya seslerin kayda alınması suretiyle ihlal etmek ve bunları TCK'nın 6/1-g maddesinde ve yukarıda belirtilen açıklamalar ışığında basın ve yayın yoluyla ifşa edilmesi suç olarak tanımlanmıştır. Buna göre örneğin birisinin evine gizli kamera yerleştirip elde edilen görüntüleri ve sesleri internet ortamında yaymak bu madde kapsamına göre cezalandırılmayı gerektirmektedir.

f. **TCK'nın 142/2-e maddesinde** belirtilen bilişim sistemleri kullanılarak yapılan nitelikli hırsızlık fiili suç olarak düzenlenmiştir.

g. **TCK'nın 158/1-f maddesinde** belirtildiği üzere bilişim sistemleri kullanılarak kişilerin dolandırılması nitelikli dolandırıcılık suçunu oluşturmaktadır. Buna göre örneğin en basit anlamda şüphelinin internet yoluyla mağdura yönelik hileli davranışlarda bulunarak onu aldatıp kendisi veya bir başkası yararına menfaat temin etmesi halinde şüpheli hakkında bu maddeye göre ceza vermek mümkün olacaktır.

h. **TCK'nın 213-218 maddeleri arasındaki 5.Bölümde** yer alan suçların yasanın 218.maddesi gereği (TCK'nın 6/1-g maddesinde ve yukarıda belirtilen açıklamalar ışığında) basın ve yayın yoluyla gerçekleştirilmesi halinde verilecek ceza yarı oranındaarttırılacaktır. Ancak, haber verme sınırlarını aşmayan ve eleştiri amacıyla yapılan düşünce açıklamaları suç oluşturmayacaktır.

i. **TCK'nın 226.maddesinde** müstehcenlik fiili düzenlenmiş olup bu maddenin kapsamına giren fiillerin (TCK'nın 6/1-g maddesindeki tanım ve yukarıda belirtilen açıklamalar ışığında) basın ve yayın yoluyla yayınlayan veya yayınlanmasına aracılık eden kişi de maddenin 2.fıkrasına göre cezalandırılacaktır. Yine maddenin 4.fıkrasına göre şiddet kullanılarak hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi cezalandırılabilecektir. Bunun dışında maddenin 5.fıkrasına göre üç ve dördüncü fıkralardaki ürünlerin içeriğini (TCK'nın 6/1-g maddesindeki tanım ve yukarıda belirtilen açıklamalar ışığında) basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini, dinlemesini veya okumasını sağlayan kişi de cezalandırılabilecektir.

j. **TCK'nın 10.Bölümünde** çalıştayın temelini teşkil eden bilişim suçları düzenlenmiştir.

Bu bölümde yer alan 243.maddenin 1.fıkrasında bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme ve orada kalmaya devam etme, 2.fıkrasında 1.fıkrada yer alan fiilin bedeli karşılığında yararlanılabilen sistemler hakkında işlenmesi, 3.fıkrasında bu fiiller nedeniyle sistemin içeriklerinin yok olması veya değişmesi fiilleri

cezai müeyyideye bağlanmıştır.

Bu bölümde yer alan 244.maddenin 1.fıkrasında bilişim sisteminin işleyişini engelleme veya bozma eylemi, 2.fıkrasında bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme fiilleri, 3.fıkrasında Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hâli cezalandırılmıştır. Maddenin 4.fıkrasında ise *"Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."* denilmek suretiyle önceki fıkralarda tanımlanan eylemler nedeniyle şüphelinin, kendisi veya bir başkası yararına sağladığı haksız çıkarın, bir başka suçu oluşturmaması hâlinde bu fıkra uyarınca cezalandırılması öngörülmüştür.

Bu bölümde yer alan 245. maddede, banka ve kredi kartlarının kötüye kullanılması suç olarak düzenlenmiştir. Belirtmek gerekir ki, bize göre bu hükmün bilişim suçu kategorisi içerisinde düzenlenmesi uygun değildir. Zîra anılan maddenin rıza dışında elde edilen banka veya kredi kartının yine kart sahibinin rızası dışında kullanılması hâlini suç saydığı görülmektedir. Bu hâli ile bu suçun aslında kartın hırsızlık, yağma veya kaybedilmesi sonucu ele geçirilmesi gibi sahibinin rızası dışında elinden çıktıktan sonra kullanılması söz konusu olduğundan, Yasa'nın 2.Kitabının 2.Kısmının 10.Bölümünde yer alan "Malvarlığına Karşı Suçlar" arasında düzenlenmesinin daha doğru olacağı kanısındayız.

k. TCK'nın 267.maddesinde iftira suçu düzenlenmiş olup bu maddenin 1.fıkrasına göre bir ihbar veya şikâyetin iftira suçunu oluşturabilmesi için yetkili makamlara yöneltilmiş olması veya basın ve yayın yoluyla yapılması gerekmektedir. Burada ilk anda ihbar veya şikâyetin basın veya yayın yoluyla yapılması halinde iftira suçunun nasıl oluşabileceği düşünülebilir. Ancak bilindiği üzere Cumhuriyet Savcıları basında yer alan herhangi bir haberi ihbar kabul ederek soruşturmaya başlaması mümkündür. Bu anlamda yazılı veya görsel basında çıkan bir haberin Cumhuriyet Savcısı tarafından ihbar kabul edilerek soruşturma konusu yapılması mümkün olduğu gibi, TCK'nın 6/1-g maddesindeki tanım ve yukarıda belirtilen açıklamalar ışığında, sosyal medyada veya internet sitelerinde yer alan bir ihbar veya şikâyetin Cumhuriyet Savcıları tarafından soruşturulmasında bir engel bulunmamaktadır. İşte bu şekilde başlayan bir soruşturmada, örneğin internet yoluyla yapılan ihbar veya şikâyetin haksız olduğu ve bunu yapan kişinin iftira kastıyla ihbar veya şikâyette bulunduğu kanısına varılır ise internette bu ihbar veya şikâyeti yapan kişi hakkında iftira suçundan ayrıca soruşturma yapılmasında bir engel yoktur.

l. TCK'nın 318/2.maddesinde halkı askerlikten soğutma fiilinin basın ve yayın yoluyla işlenmesi hâlinde verilecek cezada artırım yapılması öngörülmüştür. Belirtilmelidir ki, burada belirtilen basın veya yayın kelimeleri, TCK'nın 6/1-g maddesindeki tanım ve yukarıda belirtilen açıklamalar ışığında yazılı ve görsel basın olduğu gibi aynı zamanda elektronik kitle iletişim araçlarını da kapsamaktadır.

1.2.2. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Bu kanunda internet ortamında yapılan yayınla ilişkisi olan süjeler, bu

süjelerin sorumlulukları, bilgilendirme yükümlülüğü, erişimin engellenmesi kararı, içeriğin yayından kaldırılması ve cevap hakkı, idari yapı ve görevler düzenlenmiştir.

1.2.3. 5809 Sayılı Elektronik Haberleşme Kanunu

Bu kanunda elektronik haberleşme ilkeleri, elektronik haberleşme sektöründeki yetkili merciler, görev ve yetkileri, elektronik haberleşme sektöründe yetkilendirme, işletmecilerin hak ve yükümlülükleri, tarifeler, erişim ve ara bağlantı, geçiş hakkı, kamulaştırma, numaralandırma ve internet alan adları, spektrum yönetimi, tüketici ve son kullanıcı hakları, onaylanmış kuruluşlar ve piyasa gözetimi, denetim, kurumun yetkisi ve idari yaptırımlar ve cezai hükümler düzenlenmiştir.

1.2.4. 5070 Sayılı Elektronik İmza Kanunu

1.2.5. 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu

1.2.6. 5271 Sayılı Ceza Muhakemesi Kanunu

Hızla gelişen bilişim teknolojisinin oluşturduğu koşullarda bilgisayarlar ve bilgisayar programları hayatın önemli ve ayrılmaz bir parçası hâline gelmiştir. Pek çok kişi gibi suç işleyen kişiler de bilgisayar sistemlerini kullanmakta ve işledikleri suçlarla ilgili olarak izler bırakmaktadırlar. Delilden sanığa gitmeyi hedefleyen ve teknik delillere önem veren CMK'nın bilgisayar sistemlerinde bulunması muhtemel delillerin elde edilmesine kayıtsız kalması beklenemezdi. Bununla birlikte, bilgisayarın kişi hayatına çok yoğun biçimde girmesi nedeniyle bilgisayar sistemlerinin içerisinde kişilerin özel hayatlarına ve ticari hayatlarına ilişkin pek çok bilgi depolanmıştır. Bu nedenle bu sistemlere müdahale, bilgisayar sistemlerinde arama yapılması ve bunlara el konulması, basit el koymaya göre daha sıkı koşullara bağlanmıştır.

5271 sayılı Ceza Muhakemesi Kanunu'nun *'bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma'*, 135. maddesinde *'iletişimin tespiti, dinlenmesi ve kayda alınması'* , 140. maddesinde *'teknik araçlarla izleme'* konularında, kimi farklı hükümlere yer verilmiştir. CMK'da yer alan bu kurallar, ağırlıklı olarak, bilişim suçları dışında özel önem verilen kimi suçların veya genel olarak suçların delillendirilmesinde bilişim alanına yönelebilmeye ilişkindir.

5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesi aynen şu şekildedir:

"Madde 134 - (1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet Savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki

bütün verilerin yedeklemesi yapılır.

(4) İstemesi hâlinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."

Maddenin birinci fıkrası, Anayasa ve Siber Suçlar Sözleşmesi'ne uygun yapılandırılmış olup "Başka bir delil elde etme imkânının bulunmaması"ön şart olarak düzenlenmiştir. Yalnızca soruşturma evresinde başvurulabilen bir tedbir olmayıp rahatlıkla kovuşturma evresinde de başvurulabilecek bir yoldur.Cumhuriyet savcısının istemi gerekmektedir. Özel hayatın gizliliğine doğrudan müdahale edilen bu yönteme başvurulabilmesi için, diğer tüm olanaklara başvurulmuş olması gerekmektedir. Dolayısıyla son çare olarak bu yola başvurulması gerekir. Tedbir kararını ancak hâkim verebilir.

Madde metnindeki 'başka surette delil elde etme imkânının bulunmaması'cümlesi, arama yapabilmesinin ilk koşulunun, "başka surette delil elde etme imkânının bulunmaması"olduğunu göstermektedir. İlgili suça ilişkin kuvvetli deliller varsa, elektronik delillere ulaşılmasına gerek yoktur. Kanun koyucu, kişinin özel hayatını ve gizliliğini korumak amacıyla, elektronik deliller için "en son başvurulacak yöntem" ilkesini benimsemiştir. Ancakbu ön koşul, kişi hak ve özgürlükler açısından yerinde ise de, işin niteliği açısından sorunlara neden olabilecek yapıdadır. Misal, bir soruşturmada bilgisayarlara hemen el konulamaması veya bunlarda hemen arama yapılamaması, delillerin kaybolması sonucunu doğurabilir. Bu nedenle maddenin bu fıkrasının dar yorumlanması gerekir. Bu hususun **somut olayın özelliğine göre Cumhuriyet Savcısı tarafından değerlendirilmesi gerekir. Buna ilaveten, Kanun koyucu şüphenin derecesine yer vermediğinden, tedbirin uygulanması için basit şüphenin oluşması yeterlidir.**

CMK. önemli saydığı bir takım koruma tedbirlerini, diğer tedbirlerden ayırarak bu tedbirlere klasik soruşturma ve delil elde etme yöntemlerinin denenip bir sonuç alınamadığı durumlarda uygulanmasına imkân verilmiştir. 'İkinci derecede uygulanabilirlik' olarak da ifade edilen bu koşul, orantılılık ilkesinin somutlaşmış bir biçimidir. **Buna göre, aynı amaca hizmet eden iki koruma tedbiri var ise bu tedbirlerden daha ılımlı olan ve kişi hak ve özgürlüklerine daha az müdahale edilen tercih edilmelidir.**

CMK 134/1. madde uyarınca yalnızca şüphelinin kullandığı ve ona ait olan bilgisayar, bilgisayar kütükleri vs.de arama yapılabilinir. Şüpheli dışındaki kimselerin kullandığı veya şüphelinin kullanmamış olması kaydı ile üçüncü kişilere ait bilgisayarlarda bu koruma tedbiri uygulanamaz. Öncelikle ortada bir şüphelinin bulunması gerekir. **Üçüncü kişilere ait bilgisayarda bu koruma tedbirinin uygulanabilmesi için, şüphelinin bilgisayar veya bilgisayar kütüğünü kullanmış veya kullanıyor olması gerekir.**

Şüphelinin kullanmış olduğu bilgisayarın, başkasına ait olması durumunda da, gerekli koşulların yerine getirilmesinden sonra bilgisayarda arama yapılması mümkün olabilecektir.

Maddenin ikinci fıkrasında, bilgisayarlar ve diğer ilgili cihazlara hangi hallerde el konulacağı belirtilmiştir. Yalnızca bilgisayarın şifrelenmiş olduğunun ve gizlenmiş verilere ulaşılamamış olduğunun tespiti halinde el koyulacağının belirtilmiş olması, aygıtlara bu haller dışında el konulamayacağı anlamına gelmektedir. Madde, şifrenin çözülememesi durumunu açıklığa kavuşturmaktadır. İlgili fıkra uyarınca, bilgisayarın kendisinde, programlarında, kütüklerinde veya işletim sisteminde şifreleme mevcut olup bu şifrenin çözülememesi ve nihayetinde gizli olan verilerin incelenememesi durumunda fiziksel olarak bilgisayarın kendisine, harici belleklere veya sair araç ve gereçlere elkonulabileceği belirtilmiştir. Elkoyma işlemi geçici niteliktedir. Dolayısıyla şifrelemenin çözümlenmesi ve kopyalamanın yapılmasının ardından bu tedbire son verilir. Tüm bu işlemlerin de makul sürede yapılması gereği tartışmasızdır.

Maddenin üçüncü fıkrasında,elkoyma işlemi esnasında, sistemdeki verilerin tümünün yedeklemesinin yapılması gereği belirtilmiştir. Uygulamada yedeklemenin elkoyma işlemi sırasında değil, elkoyma işlemi sonrasında yapıldığı hususu eleştirilmektedir. Olay mahallinde yedekleme yapma imkânı, teknik ve fizikî koşulların yetersiz olması nedeniyle sağlıklı gerçekleşmeyebilir ve delillerin kaybolması sonucunu da doğurabilir. Şüphelinin kullandığı bilgisayar ve bu bilgisayarının parçaları dolayısıyla yedekleme esnasında her zaman laboratuar ortamı da müsait olmayabilir. Bunların yanında, elkoyma işleminden sonra çıkartılacak yedek sağlıklı olmayacak vesoruşturma evresi için akıllarda soru işareti bırakabilecektir. Bu nedenle yedekleme usul ve esaslarının daha ayrıntılı düzenlenmesi gerekmektedir. Burada "elkoyma işlemi sırasında' cümlesinin iyi yorumlanması gerekir. Bu durumun yalnızca olay yeri ile sınırlandırılması mümkün değildir. Dolayısıyla Yasanın amacına uygun olarak, muhafaza yapıldıktan sonra bilgisayar ve kütüklerine zarar verilmeyecek bir ortamda verilerin tespiti yapılırken yedeklemenin yapılması gerekir.

Maddenin dördüncü fıkrasında, yedeklemesi yapılan sistemdeki verilerin bir kopyasının şüpheli veya vekiline verileceği düzenlenmiştir. Belirtilen bu husus isabetli olmakla birlikte, örneğin bir çocuk pornosu suçunda, kişilerin özel fotoğraf ve videolarının bulunduğu iddiasında veya kişilere ait kredi kartı bilgilerinin yer aldığı soruşturmalarda, kopyaların şüpheliye verilmesi suçun işlenmesine devam edilmesini sağlayabileceğinden, bu gibi durumların ayrıca göz önünde bulundurulması gerekir.

Maddenin beşinci fıkrasında, soruşturma esnasında sistemin tümünün yedeklenmesinin yerine, zaman kazanmak adına yalnızca esaslı noktaların kağıda dökülmesi düzenlemiştir. İstisnai bir durumu oluşturan bu yöntem, yalnızca soruşturma ile ilgili olarak bilgisayar programlarında veya kütüklerinde bulunan çok önemli, nokta delillerin elde edilmesi hâlinde kullanılabilir. Bu esnada veri kayıplarının ve endişelerin önüne geçilmesi amacıyla verilerin "hash değeri" hesaplanarak çıkan değere ilişkin tutanak tutulabilir.

Elektronik delillerin yedeğinin alınması ve elektronik olarak mühürlenmesi, aslında şüpheliden çok delil toplayan görevlilerin faydasınadır. Zîra elektronik delillerin her an değişebileceği veya değiştirilebileceği bir ortamda, esas olarak kaygan zeminde duran kişi delil toplayan görevlidir. Bu işlemlerin yapılmadığı her delil toplamada, şüpheli veya avukatı toplanan delillerin hukuka aykırı olduğu itirazında bulunabilir, bu durumda bunun aksini ispat etmek emniyet görevlilerine düşmektedir. Bu nedenle özellikle sayısal delillerin, zamanında ve doğru şekilde toplanması çok

önemlidir. Böylece yargılamada gecikmelere neden olunmaz.

1.2.7. Fikir ve Sanat Eserleri Kanunu

1.2.8. Türk Borçlar Kanunu

1.2.9. Türk Medeni Kanunu

1.2.10. Türk Ticaret Kanunu

1.2.11. Hukuk Muhakemesi Kanunu

1.3. Yönetmelik Hükümleri

1.3.1. Adlî ve Önleme Aramaları Yönetmeliği

Adlî ve Önleme Aramaları Yönetmeliği'nin 17. maddesi "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlığını taşımakta olup şu şekilde düzenlenmiştir:

"Madde 17 - Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.

Bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.
Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir."

Bu madde, 5271 sayılı CMK'nın 134. maddesi ile paralellik taşımakla birlikte, **"bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları"** da kapsamıştır. Böylece kanunda kullanılan **"şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütükleri"** ibaresi genişletilmiştir. Fakat yeterli olmayan, eksik kalan düzenlemenin hafıza kartları, el bilgisayarları, cep telefonları, taşınır bellekler, yazıcı ve fakslar, modemler ve sair elektronik veri barındırıcılarını da kapsaması gerekir. Uygulamada "bilgisayar" dan anlaşılan ve çoğunlukla tek başına elkonulan bilgisayar kasası, yalnızca bilgisayarın bir

birimi olup tamamı değildir. Tek başına suç vasıtası sıfatını haiz olamayacak bilgisayar kasası yerine, bilgisayara ait tüm birimlerin incelenmesi veya zaruri durumda bu birimlere el konulması gerekmektedir.

1.3.2. Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik

Talih oyunlarının kanun dışı olarak sanal ortam üzerinden oynatılmasının takibi ve denetlenmesi, ilan ve reklamlarının önlenmesine dair usul ve esasları düzenleyen yönetmelik 26108 sayılı Resmî Gazete'de 14.03.2006 tarihinde yayınlanmıştır.

1.3.3. Elektronik Haberleşme Güvenliği Yönetmeliği

Elektronik haberleşme güvenliğine ilişkin usul ve esasları düzenleyen yönetmelik, 26942 sayılı Resmî Gazete'de 20.07.2008 tarihinde yayınlanmıştır.

1.3.4. Elektronik Kimlik Bilgisini Haiz Cihazlara Dair Yönetmelik

Elektronik kimlik bilgisini haiz cihazların kayıt altına alınmasına, kayıp, kaçak veya çalıntı cihazlara elektronik haberleşme hizmeti verilmesinin engellenmesine ve elektronik kimlik bilgisi değiştirilen cihazlara ilişkin usul ve esasları düzenleyen yönetmelik, 27271 sayılı Resmî Gazete'de 27.06.2009 tarihinde yayınlanmıştır.

1.3.5. Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik

Kodlu veya kriptolu haberleşme sistemi üretimi, başvuru esasları, değerlendirilmesi, izin işlemleri, emniyet ve muhafaza tedbirleri, denetim, müeyyide ve kayıtlarının tutulmasında uygulanacak usul ve esaslar ile yapılacak iş ve işlemleri belirleyen yönetmelik, 27738 sayılı Resmî Gazete'de 23.10.2010 tarihinde yayınlanmıştır.

1.3.6. Kayıtlı Elektronik Posta Sistemine İlişkin Usul Ve Esaslar Hakkında Yönetmelik

Kayıtlı elektronik posta sisteminin hukukî ve teknik yönleri ile işleyişine ilişkin usul ve esasları düzenleyen yönetmelik, 28036 sayılı Resmî Gazete'de 25.08.2011 tarihinde yayınlanmıştır.

1.3.7. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

Elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenleyen yönetmelik, 28363 sayılı Resmî Gazetede 24.07.2012 tarihinde yayınlanmıştır.

1.3.8. Adalet Bakanlığı Bilgi Sistemlerinin İnternet Üzerinden Gelecek Tehlikelerden Korunması ve Veri Güvenliğinin Sağlanmasında Uyulacak Usul ve Esaslar Hakkında Yönetmelik

Adalet Bakanlığına ait bilgi sistemlerinin internet üzerinden gelecek tehlikelerden korunması ve veri güvenliğinin sağlanması için alınacak güvenlik önlemlerine ilişkin usul ve esasları düzenleyen yönetmelik, Resmî Gazete'de yayınlanmamıştır.

1.3.9. İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik

İnternet toplu kullanım sağlayıcıları ve ticari amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri ve sorumlulukları ile denetimlerine ilişkin esas ve usulleri düzenleyen yönetmelik 26687 sayılı Resmî Gazete'de 01/11/2007 tarihinde yayınlanmıştır.

1.3.10.İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik

İçerik sağlayıcıların, yer sağlayıcıların ve erişim sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenleyen yönetmelik 26716 sayılı Resmî Gazete'de 30/11/2007 tarihinde yayınlanmıştır.

1.3.11.İnternet Alan Adları Yönetmeliği

".tr" uzantılı internet alan adları yönetimine ilişkin usul ve esasları düzenleyen yönetmelik 27752 sayılı Resmî Gazete'de 07/11/2010 tarihinde yayınlanmıştır.

1.4. Tebliğ Hükümleri

1.4.1. Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

Elektronik imzaya ilişkin süreçleri ve teknik kriterleri detaylı olarak belirleyen tebliğ, 25692 sayılı Resmî Gazete'de 06/01/2005 tarihinde yayınlanmıştır.

1.4.2. Kayıtlı Elektronik Posta Sistemi İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

Kayıtlı elektronik posta sistemine ilişkin süreçleri ve teknik kriterleri detaylı olarak belirleyen tebliğ 28036 sayılı Resmî Gazete'de 25/08/2011 tarihinde yayınlanmıştır.

1.4.3. Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ

Kayıtlı elektronik posta hesabı adreslerinin yapısına ve kayıtlı elektronik posta rehberinin oluşturulmasına, güncellenmesine, işletilmesine ve kullanılmasına ilişkin usul ve esasları belirleyen tebliğ, 28294 sayılı Resmî Gazete'de 16/05/2012 tarihinde yayınlanmıştır.

2 KAVRAMLAR

2.1. Bilişim Sistemi
2.2. Bilgisayar
2.3. Veri
2.4. Elektronik Veri
2.5. IP (internet protocol) Adresi
2.6. Ethernet Kartı
2.7. MAC (media access control) Adresi
2.8. Bilgisayar Kütüğü
2.9. Sunucu Kütüğü
2.10. Bilgisayar Programı
2.11. RAM (Random Access Memory)
2.12. İmaj Alma ve Hash Değeri
2.13. Bilişim Ağı (network), internet, internet ortamı, intranet, bulut bilişim (cloud computing)
2.14. Geniş Alan Ağı (wAN), Yerel Alan Ağı (LAN)
2.15. Etki Alanı (Domain Name)
2.16. Yer Sağlayıcı, İçerik Sağlayıcı, Servis / Erişim Sağlayıcı, Toplu Kullanım Sağlayıcı, Elektronik Sertifika Hizmet Sağlayıcısı
2.17. Trafik Bilgisi (Log Kayıtları)
2.18. Suç İşlemede Kullanılan Teknik Araçlar ve Yöntemler
2.19. DNS (Domain Name System - Alan Adı Sistemi)
2.20. Sunucu
2.21. İnternet Ortamı
2.22. İnternet Ortamında Yapılan Yayın
2.23. Erişim
2.24. Bilgi
2.25. Cracker
2.26. Hacker

2. KAVRAMLAR

2.1. Bilişim Sistemi

Bilgisayar, çevre birimleri (bir bilgisayarın çalışması için zorunlu olmayan ancak kullanımını kolaylaştıran hoparlör, CD ROM, mouse, klavye, kulaklık, yazıcı vb), iletişim altyapısı (elektronik haberleşme, internet, intranet gibi) ve programlardan oluşan veri işleme saklama ve iletmeye yönelik sistemi ifade eder.

2.2. Bilgisayar

Belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen masaüstü, dizüstü bilgisayarlar, cep telefonu ve benzeri tüm elektronik araçları ifade eder.

Bilgisayarın elektronik kısmına donanım (Hardware), program kısmına ise yazılım (Software) denir. Bilgisayarda 4 unsur bulunmaktadır: Bunlar;

a) Bilginin girişi (giriş birimleri: klavye, fare, kamera, scanner yani tarayıcı, fax-modem),
b) Bilginin saklanması (hafıza: hard disk, disket, CD, DVD, USB, harici hard disk, bulut bilişim vb.),
c) Bilginin işlenmesi (beyin: merkezi işlem birimi yani CPU),
ç) Bilginin çıkışı (çıkış birimleri: monitör yani ekran, yazıcı, çizici, modem gibi).

2.3. Veri

Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri ifade eder (bkz. 5651 Sk'nun 2/a mad.).

2.4. Elektronik Veri

Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları ifade eder (bkz. 5070 Sk'nun 3/a mad.)

2.5. IP (Internet Protocol) Adresi

Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleri ile iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, internet protokolü standartlarına göre verilen adresi ifade eder.

İnternete bağlanan her bilgisayara internet servis sağlayıcı tarafından bir IP adresi atanır ve internetteki diğer bilgisayarlar bu bilgisayara verilen IP adres ile ulaşırlar.

IP adresleri, dinamik ve statik olarak iki bölüme ayrılır. Genel olarak dinamik IP adresi kullanılır. Dinamik IP adresleri, zamana ve oturuma göre değişir. Çünkü servis sağlayıcı o an için boş olan IP adresini kullanıcıya atar. Statik IP adresi ise, zamana ve oturuma göre değişmeyen adresi ifade eder. Ancak sistem yöneticisi tarafından tanımlanıp değiştirilebilir.

IP, 0 ile 255 sayıları arasında değişen, genellikle noktalı onluk (desimal) formatta gösterilen 32 bitlik adreslerdir. Örneğin, 155.212.56.73.

Adlî bilişim terminolojisinde RAM'de bulunan kanıtlar uçucu delil olarak adlandırılır. Bunun sebebi, sistemin kapatılması veya enerjinin kesilmesi ile RAM'de bulunan verlerin kaybolmasıdır.

Ayrıca alan adları için de bir IP adresi vardır. Bir internet sayfasını yazdığımız kısmına (ağ tarayıcı) bu IP adresi de yazılarak bağlanılabilir. Ancak bu rakamları yazmak pratik ve akılda kalıcı olmadığından alan adı IP adresine karşılık gelen bir alan adı sistemi kullanılmaktadır.

2.6. Ethernet Kartı

Network (ağ) sistemlerinde kullanılan, bilgisayarla ağ arasında iletişimi sağlayan ağ ara birim kartıdır. Her Ethernet kartının MAC adresi vardır. Bu adres, 00-23-c3-45-00-b3 şeklindedir. Ethernet kartı iletilecek olan verileri, paketlere böler ve kart çıkışına bağlı ağ kablosuna gönderir.

2.7. MAC (Media Access Control) Adresi

Ethernet ağında sistemler birbirlerinden sahip oldukları MAC adresi ile ayırt edilirler. Ethernet, wi-fi, bluetooth gibi ortamlarda ağ donanımını tanımlamaya yarayan, bir bilgisayarın ethernet kartına üretici tarafından kodlanmış fiziksel adres bilgileri ifade eder. Her Ethernet kartının dünyada eşi olmayan bir adrese sahiptir. Örneğin; bir notebook bilgisayarda modem kablolu Ethernet ve wireless (wi-fi) Ethernet varsa üç ayrı MAC adresi vardır.

Bant genişliği nedir?
Bir telefon hattı, kablo hattı, uydu beslemesi vb. ile taşınabilecek bilgi miktarıdır. Bant genişliği ne kadar büyükse bağlantınızın hızı o kadar fazladır ve İnternet deneyiminiz daha hızlı indirmeli ve TV tarzı bir deneyime o kadar yakın olur.

2.8. Bilgisayar Kütüğü

Bilgisayarın ve bilgisayarda yer alan dosyaların, geçirdiği safahatlara dair kayıtların tutulduğu verileri ifade eder.

2.9. Sunucu Kütüğü

Bir sunucudaki bütün değişikliklerin kayıt altına alındığı kütük dosyasını ifade eder. Kütüklerde bilgisayar ağına erişim, dosyalarda yapılan değişikler, veri indirme ve yükleme gibi kayıtlar tutulur.

2.10. Bilgisayar Programı

Bilgisayara bir işi yaptırmak için verilen komutlar bütününe bilgisayar programı denir. Bilgisayar programı bir programlama dili kullanılarak yazılır. Program çalıştırıldığında bilgisayar ilgili komutları okuyarak programda kendisine tarif edilen işi yapar.

MAC, 48 bit'lik bir adres olduğundan dolayı 248 = 281, 474, 976, 710, 656 değişik ağ kartını tanımlamak için kullanılabilir. Örnek bir MAC adresi: 01: 23: 45: 67: 89: AB. (www.wikipedia.com)

2.11. RAM (Random Access Memory)

Rastgele erişimli bellek demektir. Birbirinden bağımsız hafıza hücrelerinden oluşur. Veri depolanabilir, silinebilir, okunabilir, değiştirilebilir. Bilgisayar çalıştığı sürece RAM faaliyetine devam eder. Bilgisayar kapandığında ise RAM' de depolanmış veriler silinir.

2.12. İmaj Alma Ve Hash Değeri

İmaj Alma, veri depolama cihazlarının sektör bazında başka bir veri depolama cihazına kopyalanması işlemini ifade eder.

Hash Değeri, dosyaların parmak izi olarak nitelendirilebilir. Dosyalar çeşitli karmaşık algoritmalar ile taranır ve dosyanın benzersiz bir parmak izi çıkarılır. Adlî bilişimde geçen bir zaman sürecinde bir depolama alanındaki bilgiler üzerinde değişiklik olup olmadığının anlaşılması için kullanılır. Dataya ilişkin olarak yapılan işlemler öncesinde ve sonrasında datanın hash değeri alınır. Eğer hash değeri işlem öncesinde ve sonrasında aynı ise datada herhangi bir değişiklik olmadığı, eğer hash değeri farklı ise datada değişiklik olduğu sonucuna varılabilir. Ancak bunun istisnaları da söz konusudur. Örneğin, bozuk sektörler sonucu alınan imajlarda ilk hash işleminden sonra "bad sektör" oluşması halinde doğal olarak belirli bir zaman sonra ikinci hash işleminde hash değeri farklı çıkar. Bir diğer istisna da RAM arızasıdır. Ayrıca kullanılan donanımların bozulması veya arızalı olmaları veya elektriksel sorunlar sebebiyle de hash değeri farklı çıkabilir. Kolluk kuvvetleri bu nedenle uygulamada hash değerinin farklı çıkmasını ve olası tartışmaları önlemek için bilgisayarların imajlarını kendi birimlerinde almayı tercih etmektedir.

2.13. Bilişim Ağı (Network), Internet, Internet Ortamı, Intranet, Bulut Bilişim (Cloud Computıng)

Bilişim Ağı (Network); bilgisayarların birbirlerine bağlanması ile oluşan yapıyı,

Internet, dünya genelindeki bilgisayar ağlarını ve kurumsal bilgisayar sistemlerini birbirlerine bağlayan elektronik iletişim ağını,

Internet ortamı, haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

Intranet, sadece belirli bir kuruluş içerisindeki bilgisayarları yerel ağları ve geniş alan ağlarını birbirlerine bağlayan ağı,

Bulut Bilişim (Cloud Computing); bilişim aygıtları arasında ortak bilgi paylaşımı sağlayan hizmetlere verilen genel ismi ifade eder.

2.14. Geniş Alan Ağı (WAN), Yerel Alan Ağı (LAN)

Geniş Alan Ağı, birden fazla cihazın birbirleri ile iletişim kurmasını sağlayan fiziksel veya mantıksal büyük ağı ifade eder. Yerel alan ağlarının birbirlerine bağlanmasını sağlayan çok geniş ağlardır. En meşhur geniş alan ağı internettir.

Yerel Alan Ağı; ev, okul, işyerleri gibi sınırlı coğrafi alanda bilgisayarları ve araçları birbirlerine bağlayan bilgisayar ağını ifade eder.

2.15. Etki Alanı (Domain Name)

Bir web sitesinin internetteki adı ve adresidir. Bunlar bilgisayar ortamında nümeriktir, ancak akılda kalması ve kolay kullanım açısından anlamlı kelimelere dönüştürülmüştür.

.com
Ticari kuruluşlar için

.net
Çalışma alanı internet olan kuruluşlar için

.org
Dernekler, Organizasyonlar için

.gov
Devlet kuruluşları için

.edu
Eğitim kuruluşları için

.mil
Askeri kuruluşlar için

.ac
Akademik kuruluşlar

(Bazı ülkelerde karşılığı **.edu** dur) için domain uzantılarıdır.

2.16. Yer Sağlayıcı, İçerik Sağlayıcı, Servis / Erişim Sağlayıcı, Toplu Kullanım Sağlayıcı, Elektronik Sertifika Hizmet Sağlayıcısı

İçerik sağlayıcı, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

Yer sağlayıcı, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,

Servis / Erişim sağlayıcı, Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

Toplu kullanım sağlayıcı, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan kişileri,

Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri, ifade eder.

2.17. Trafik Bilgisi (Log Kayıtları)

İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri ifade eder.

Yer sağlayıcı trafik bilgisi, internet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgileri,

Erişim sağlayıcı trafik bilgisi, internet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileriifade eder.

Telekomünikasyon İletişim Başkanlığı tarafından hazırlanan IP Log İmzalayıcı programı yayımlanmıştır. IP Log İmzalayıcı, dahili IP dağıtım loglarının doğruluk ve bütünlüğünün korunması için, bu log dosyalarının girdi olarak alınarak, elektronik imzasının oluşturulması ve bu dosyaların imzası ile birlikte saklanması amacıyla geliştirilmiştir. (http://www.tib.gov.tr/tr/tr-menu-55-ip_log_imzalayici_programi.html)

2.18. Suç İşlemede Kullanılan Teknik Araçlar Ve Yöntemler

2.18.1.Virüs

Bilgisayar virüsleri, bir bilgisayardan diğerine yayılmak ve bilgisayarın çalışmasına müdahale etmek amacıyla tasarlanmış küçük yazılım programlarıdır.

Bir virüs, bilgisayarınızdaki verileri bozabilir veya silebilir, kendisini diğer bilgisayarlara yaymak için e-posta programınızı kullanabilir veya sabit diskinizdeki her şeyi silebilir.

Bilgisayar virüsleri genelde e-posta mesajlarındaki eklerle veya anlık mesajlaşma ile yayılır. Bu nedenle, e-posta eklerinin, mesajın kimden geldiğinin bilinmediği veya böyle bir ek geleceğinin bilinmediği durumlarda asla açılmaması önemlidir. Virüsler, komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler hâlinde kimliklerini gizleyebilirler.

Bilgisayar virüsleri ayrıca Internet'ten yapılan karşıdan yüklemeler yoluyla da yayılır. Yasalara aykırı yazılımlarda veya karşıdan yüklemek istenilen diğer dosyalar veya programlarda gizlenebilirler.

2.18.2.Truva Atı (Trojan)

Yararlı gibi görünen; ancak aslında zarara yol açan bilgisayar programlarıdır. Truva atları, insanların, meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya yöneltilmeleri yoluyla yayılır. Truva atları, ücretsiz olarak yüklenilen yazılımlarda da bulunabilir. Güvenilmeyen bir kaynaktan asla yazılım yüklenmemlidir.

Trojan, "kurban"ının tahmin etmediği bir şekilde ve isteği olmaksızın, gizli ve genellikle kötü amaçlı bir faaliyette bulunan bir programdır. Her ne kadar evrensel olarak kabul görmemişse, de,virüstenfarkının kendi kendini çoğaltması olduğu söylenebilir.

2.18.3.Solucan

Solucan da, virüs gibi, kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır ve bunu otomatik olarak yapar. İlk olarak, bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir. Solucan bir kez sisteminize girdikten sonra kendi başına ilerleyebilir.

Solucanların en büyük tehlikesi, kendilerini büyük sayılarda çoğaltma becerileridir. Örneğin bir solucan, e-posta adres defterinizdeki herkese kopyalarını gönderebilir ve sonra aynı şeyi onların bilgisayarları da yapabilir. Bu domino etkisinin getirdiği yoğun ağ trafiği iş yeriiş yeri ağlarını ve Internet'in tümünü yavaşlatabilir.
Yeni solucanlar ilk ortaya çıktıklarında çok hızlı yayılırlar. Ağları kilitlerler ve kullanıcıların Internet'teki Web sayfalarını görüntülerken uzun süreler beklemelerine yol açarlar.

Solucan, virüslerin bir alt sınıfıdır. Bir solucan genellikle kullanıcı eylemi olmaksızın yayılır ve kendisinin tam kopyalarını (olasılıkla değiştirilmiş) ağlardan ağlara dağıtır. Bir solucan, bellek veya ağ bant genişliğini tüketebilir, bu da bilgisayarın çökmesine yol açabilir.

Solucanlar yayılmak için bir "taşıyıcı" programa veya dosyaya gereksinim duymadıklarından, sistemde bir tünel de açabilir ve başka birinin uzaktan bilgisayarın denetimini eline geçirmesini sağlayabilir. Yakın geçmişteki solucanlara örnek olarak Sasser solucanı ve Blaster solucanı verilebilir.

Internetteki Solucan Örnekleri:

İnternette sörf yaparken karşımıza çıkan küçük pencerelerde ilgi çekici şeyler bulunmaktadır. Bunlara tıkladığımızda internet tarayıcısı (İnternet Explorer, Firefox vb.) solucan virüsü taşıyan dosyalar indirir. Tıkladığımız andan itibaren virüs

bilgisayarımızda etkinleşir. Bazı penceredeki yazıların örnekleri;

- Tebrikler 250 SMS kazandınız telefonunuza indirmek için tıklayınız.
- Tebrikler Amerika'ya gitme hakkını yakalamak için ücretsiz çekiliş kazandınız.
- Tebrikler Amerika kapınızda.
- Visa kartınıza bonus kazandınız.
- Sitemize giren 1.000.000. kişisiniz. Bizden hediye şarkı kazandınız.
- Bugün şanslı gününüzdesiniz. Bizden para ödülü kazandınız.
- Tebrikler bizden saat kazandınız.

2.18.4.Dos ve DDos Atakları

Dos, yani açılımı Denial of Sevice olan bu saldırı çeşidi bir hizmet aksatma yöntemidir. Bir kişinin bir sisteme düzenli veya arka arkaya yaptığı saldırılar sonucunda hedef sistemin kimseye hizmet veremez hale gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlayan bir saldırı çeşididir. Birçok yöntemle hizmet aksatma saldırıları gerçekleştirilebilir.

DDos ise, bir saldırganın daha önceden tasarladığı bir çok makine üzerinden hedef bilgisayara saldırı yaparak hedef sistemin kimseye hizmet veremez hale gelmesini amaçlayan bir saldırı çeşididir. Koordineli olarak yapılan bu işlem hem saldırının boyutunu artırır hem de saldırıyı yapan kişinin gizlenmesini sağlar. Bu işlemleri yapan araçlara "zombie" denir. Bu saldırı çeşidinde saldırganı bulmak zorlaşır. Çünkü saldırının merkezinde bulunan saldırgan aslında saldırıya katılmaz. Sadece diğer ip numaralarını yönlendirir. Eğer saldırı bir tek IP adresinden yapılırsa bir Firewall bunu rahatlıkla engelleyebilir. Fakat saldırının daha yüksek sayıdaki IP adresinden gelmesi Firewall un devre dışı kalmasını sağlar (Log taşması firewall servislerini durdurur). İşte bu özelliği onu DoS sadırısından ayıran en önemli özelliğidir.

2.18.5.Phising Saldırıları

Phishing "Password" (Şifre) ve "Fishing" (Balık avlamak) sözcüklerinin birleştirilmesiyle oluşturulan, Türkçe'ye yemleme (oltalama) olarak çevrilmiş bir saldırı çeşididir. Phishing saldırıları son zamanların en gözde saldırı çeşidi olarak karşımıza çıkmaktadır. Yemleme yöntemi kullanılarak bilgisayar kullanıcıları her yıl milyarlarca dolar zarara uğratılmaktadır. Yemleme genelde bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmek amacıyla kullanılır. Bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilir. Phishing saldırıları için 'bankalar, sosyal paylaşım siteleri, mail servisleri, online oyunlar vb. sahte web sayfaları hazırlanmaktır. Bu web sayfalarıyla bilgisayar kullanıcılarının özlük bilgileri, kart numarası, şifresi gibi bilgiler istenir. E-posta ve sahte sitedeki talepleri dikkate alan kullanıcıların bilgileri çalınır.

Burada şunu da belirtmek gerekir, arama motorlarında bazı bankaların dolandırıcılar tarafından hazırlanan sahte web adreslerinin yer aldığı göz önüne alınırsa, bu saldırıların yaygın olduğu görülmektedir. Tedbir olarak banka adreslerinin, adres çubuğuna elle (manuel) olarak yazılması önerilebilir.

2.18.6.Parola Kırma Saldırıları

Bir bilgisayar sisteminden iletilen ya da bir bilgisayarda saklanan verilerin

şifresini kurtarma veya öğrenme işlemine şifre kırma denir. Bu konuya genel yaklaşım, bütün tahminleri tek tek denemektir. Şifre kırma işlemi, bilgisayar şifresini unutan insanlar için yardımcı olabilir. Şifre kırma işlemi ayrıca dijital dünyada gizli verilere erişim olanağı da sağlar.

Bir şifreyi kırmak için gereken zaman şifrenin uzunluğuna ve karmaşıklığına göre değişebilir, bu ölçüm aslında şifrenin entropy'sinden sağlanır, yani şifre içinde sadece harf ve sayılar değil ^%&/();? gibi karakterler de kullanılırsa şifrenin karmaşıklığı artar. "Brute-force cracking" ismi verilen "kaba-kuvvet saldırıları" ile bir şifrenin olabilecek bütün şifre olasılıkları tahmin edilir ve denenir. Bu denemelerden birisi mutlaka gerçek şifreyi yakalar. En çok kullanılan şifre kırma yöntemleri –örneğin, sözlük atağı (dictionary attacks), Pattern Checking, Kelime listesi yerine koyma yöntemi v.b. yöntemler – deneme sayısını azaltır ve genelde Brute-Force ataktan önce kullanılır.

2.18.7.Bilişim Korsanlığı

Yukarıda açıkladığımız ve bilişim sistemleri konusundaki uzmanlıklarını suç işlemek için kullanan kişilerin yanında bir de bu bilgilerini sistemlerin güvenliğini test etmek için kullanan kişiler bulunmaktadır. Bilişim sistemlerinin, bilişim korsanları tarafından kolayca aşılıp sistemin içine girilmesi ve çeşitli eylemlerin yapılmasının nasıl olduğunun anlaşılması ve bunlara karşı önlem alınması, bu kişilerden destek alınmadan yapılması oldukça zordur. Nitekim pek çok şirket bilişim korsanlarının kendi sistemleri içinde işledikleri suçlar hakkında ilgili makamlara ihbarda bulunmamakta ve müşterilerini kaybetmektense, sessiz kalıp kayıplarına katlanmayı tercih etmektedirler.

Bu zorlukların aşılmasında, eskiden bilişim korsanlığı yapmış kişilerin bilgi ve deneyiminden yararlanma yoluna gidilmektedir. Bilişim sistemlerinin güvenliğinin bilişim korsanlığı yapmamış kişilere denetlettirilmesinden yeterince faydalı sonuçlar alınamamıştır. Uzman kişi, bilişim sisteminin saldırı karşısındaki güvenliğini, en fazla hayal gücünü zorlayarak veya bu konuda edindiği bilgileri uygulayarak test edebilmektedir. Çünkü bilişim güvenliği uzmanı, aslında bir bilişim korsanı olmadığı için kendisini bu konuda zorlasa dahi bir bilişim korsanı gibi düşünüp hareket edemez. Bilişim güvenliği uzmanları, bilişim sisteminin güvenliğini denetlerken, gerçek bir bilişim korsanının suç işleme esnasındaki psikolojik durumu içinde düşünüp sisteme karşı ani saldırılar yapamaz. Oysa önemli olan, bilişim sisteminin gerçek bir bilişim korsanı saldırısı karşısında güvenlik önlemlerinin kontrol edilmesidir. Her ne kadar bilişim güvenliği uzmanı bu testi gerçekleştirebilirse de bu test hiçbir zaman bir bilişim korsanınınki gibi olamaz. Bu ihtiyaçtan hareketle artık suç işlemeyi bırakmış eski bilişim korsanları bu testler için kullanılmakta ve bunlara *"ethical hacker (ahlâklı bilişim korsanı)"* denilmektedir.

2.18.8.Botnet Saldırısı

Bir kişi, emri altında zombi PC'lerden oluşan bir orduya sahipse bu orduya "botnet" adı verilir. BotNet ile suçlular ana bilgisayarlarıyla diğer bilgisayarlara virüsler göndermekte ve(zombi denilen) virüslü bilgisayarları esir almaktadırlar.

Diğer taraftan bu yüz binlerce bilgisayarı aynı zamanda yönetebilmekte ve tek bir hedefe örneğin 200,000 bilgisayarın gücüyle tek bir hedef için- saldırmaktadır. Botnet sunucularını yönetenler kendilerine

Botnet "robot" kelimesinin ve network kelimesinin "net""i kullanılarak oluşturulmuştur.

köle ettiği bilgisayarlardaki kayda değer tüm bilgileri (hesap bilgileri, şifreler, projeler, dosyalar, programlar, kişisel veriler) çalabilmektedirler.

2.18.9.Çöpe Dalma

"Çöplenme" veya "atık toplama" olarak da adlandırılan "çöpe dalma" yönteminde, bilişim sisteminde gerçekleştirilen bir veri-işlemi sonrasında artakalan bilgiler toplanmaktadır.

Bu bilgiler öncelikle, çıktı birimlerince üretilen ve daha sonra çöpe atılan kağıt, mürekkep şeridi gibi malzemeler üzerinde kalan bilgilerin toplanmasıyla veya bilişim sisteminin belleğinde bulunan ve ihtiyaç duyulmayan silinmiş bilgilerin gelişmiş yöntemlerle tekrar geri getirilmesiyle elde edilmektedir.

2.18.10. Gizlice Dinleme

Gizli dinleme, bilişim sistemlerinin veri taşımada kullandığı ağlara girilmesi veya bilişim sistemlerinin yaydığı elektromanyetik dalgaların yakalanması ile verilerin elde edilmesidir. Bilgisayar monitörlerinin yaydığı elektromanyetik dalgaların yakalanarak tekrar ekran görüntüsüne dönüştürülmesi, bilişim sistemlerinin merkezlerine yerleştirilecek elektromanyetik dalgaları yakalayabilen radyo vericileri aracılığı ile verilerin elde edilmesi, araya konulan yükselticiler vasıtasıyla, elektromanyetik dalgaların çok uzaklardan yakalanarak verilerin elde edilmesi, kullanılan ağlara veri gönderimi sırasında yapılan fiziksel müdahaleler sonucu, ağ üzerinde akan verilerin elde edilmesi şeklinde gizli dinleme yapılabilmektedir.

2.18.11. Veri Aldatmacası

Veri aldatmacası, veri sistemlerine veri girişi yapılırken, kasıtlı olarak yanlış verilerin girilmesi veya verilerin girildikten sonra değiştirilmesidir.
Veri aldatmacası olarak veri-işlem dokümanlarının tahrif edilmesi, veri saklama ortamında saklanan verilerin özel araçlar ile değiştirilmesi, verilere ek başka verilerin kaydedilmesi, bazı verilerin silinmesi veya kontrol aşamalarında gösterilmemesi usulleri sayılabilir.

Verilerin oluşturulması, kaydedilmesi, işlenmesi esnasında nezaret eden, verileri nakleden, kontrol eden veya şifreleyen kişiler bu suçu işleyebilmektedirler.
Herhangi bir ağ üzerindeki bilişim sistemlerine ulaşabilen kişiler de güvenlik önlemlerini aşarak bu suçu işleyebilirler.

2.18.12. Tarama

Tarama, değeri her seferinde, sıralı bir diziyi takip ederek değişen verilerin,hızlı bir şekilde bilişim sistemlerine girilmek suretiyle, sistemin olumlu cevap verdiği durumların raporlanması için yapılan işlemlerdir.

İşlem her seferinde bir numara artırılarak tekrar edilir.Böylelikle belirli bir aralıkta bulunan bilişim sistemleri tespit edilmiş olur. Aynı yöntem, internete bağlı IP adres numaralarını veya IP adresleri üzerinde açık olan portları bulmaya yönelik olarak da kullanılmaktadır.

Özellikle port taraması, son zamanlarda bilişim suçlularının sıkca başvurdukları yöntemlerden biridir. Burada kullanılan port, bilgisayarlarda bulunan fiziksel seri ve paralel portların dışında kalan mantıksal portları ifade etmektedir. Her IP Adresi portlara yani sanal veri yollarına bölünmüştür. Bu sayede aynı anda, aynı IP Adresinden farklı programlarla veri alışverişi yapılabilmektedir. Port taramasıyla karşı sisteme ait bilgiler elde edilerek sistemin açıklıkları bulunabilmektedir. Şifre ile korunmuş sistemlerin şifrelerini çözmek amacıyla da şifre taraması yapılmaktadır. Özellikle sözlüklerden seçilmiş kelimeler, sadece rakamlardan veya sadece harflerden oluşan basit şifreler, şifre taraması yapan programlar tarafından rahatlıkla çözülebilmektedir. Tarama programları internet aracılığı ile kolaylıkla bulunabilmektedir. Şifre tarayıcı programlar, geçerli şifreyi bulmak için veritabanında bulunan kelimeleri ve harf dizilerini birer birer deneyerek sistemin yanıtlarını kontrol etmektedirler. Veritabanı mantıklı kelimelerden başlamak üzere,dünya genelinde en çok kullanılan şifrelerden oluşan bir sözlük niteliğindedir.

2.18.13. Süper Darbe

Bilişim sistemlerinin, çeşitli sebeplerle işlemez hale geldiğinde, çok kısa bir süre içerisinde sistemin tekrar çalışmasını sağlamak üzere tüm güvenlik kontrollerini aşarak sistemde değişiklik yapılabilmesini sağlayan programlardır.

İlk olarak bilgisayarlarda herhangi bir programın disketten diskete kopyalanmasına engel olan "kopya koruma" yazılımlarını atlatan bir program olarak ortaya çıkmıştır.

Süper darbe programları, bilişim sistemlerinde büyük çapta tahribat yapmak isteyen bilişim suçlularına, tüm güvenlik önlemlerinden serbestçe geçebilmesinden dolayı çok geniş bir imkân sağlamaktadır.

2.18.14. Salam Tekniği

Bu teknik genellikle bankaların bilişim sistemlerinde gerçekleştirilen hukuka aykırı yarar sağlama suçları için kullanılan etkin bir yöntemdir. Sistemin esası çok fazla kaynaktan (örneğin çok sayıda banka hesabından) kaynak başına çok az miktarda hukuka aykırı yarar sağlanması esasına dayanır. Böylelikle banka ya da hesap sahipleri hesaplarda meydana gelen yetkisiz hareketi kolaylıkla fark edememekte, ancak küçük miktarların çok sayıda kaynaktan toplanmış olması fail açısından büyük miktarda bir hukuka aykırı yarar sağlamaktadır. Bu tekniğin gerçekleştirilmesi için de genellikle truva atı yazılımının çeşitleri veya benzer işleve sahip yazılımlar kullanılmaktadır.[1]

Çok sık örnek verilen bir olayda, bir banka çalışanı, bankanın tuttuğu milyonlarca mevduat hesabının dört ayda bir yapılan faiz ödemelerinin dört ondalık kesir puanına kadar hesaplandığı, sonra da aşağı veya yukarı yuvarlandığını fark etmiştir. Bankanın bilişimsisteminde bulunan yazılımuyarınca bir doların 0,0075 kadar üstünde olan her rakam bir üst sente yuvarlanmakta ve mudiye ödeme yapılmaktadır; bunun altında kalan rakamlar ise aşağı yuvarlanmakta ve bankanın hesabına eklenmektedir. Banka memuru bu işleyişi kavrayınca, sistemin yaptığı işlemi değiştiren bir yazılım yapmış ve aşağı yuvarlanarak bankanın hesabına gitmesi yerine kendi açtığı bir hesaba gitmesini sağlamıştır. Banka memurunun bu işlemi üç yıl süreyle uyguladığı ve bu

1 Dülger, s.105.

süre içinde milyonlarca dolar tutarında hukuka aykırı yarar sağladığı belirtilmektedir.[2]

2.18.15. Tavşanlar

Tavşan olarak adlandırılan yazılımlar, adını aldıkları hayvan gibi çok hızlı üreyebilmektedirler. Bunlar içine girdikleri bilişim sisteminin içinde işlemciye sürekli anlamsız komutlar vererek işlemcinin bilişim sisteminin normal işleyişini sağlayan komutları vermesini engellemekte ve giderek sistemin yavaş çalışmasına neden olarak en sonunda sistemi çalışamaz hale getirmektedirler.[3]

Tavşanlar genellikle çok kullanıcılı geniş sistemlerin işleyişini bozmak ve veri iletim ağını koparmak amacıyla kullanılan bir yazılım türüdür. İngiltere'de gerçekleşen bir olayda "Mad Hacker" takma adlı bir bilişim korsanı Queen Mary Üniversitesi'nin ve Hull Üniversitesi'nin bilişim sistemlerine yüklediği tavşan yazılımları sayesinde bu sistemlerin durmaksızın "Sanırım benim çılgın olduğumu biliyorsunuzdur... Ayrıca bunalımdayım" ve "Meydan okuduğunuzu görüyorum" yazılarını yazmasını sağlayarak sistemlerin işlevsiz hâle gelmesini sağlamıştır.

2.18.16. Gizli Kapılar

Tuzak kapısı, arka kapı ya da açık kapı da denilen gizli kapılar, bir sistemin yazılımını yapan kişi tarafından, yazılımın içine gizli bir şekilde yerleştirilen bir virüs yazılımıdır.Bu programın çalıştığı bilgisayara virüsü yerleştiren kişi uzaktan erişim yöntemiyle sistem kontrollerine yakalanmadan bilişim sistemine sızabilmektedir. Adından da anlaşılacağı üzere uygulamayı geliştiren şirket ya da kişi tarafından bilinçli bir şekilde bırakılmış açık noktalardır.

2.18.17. Eş Zamansız Saldırılar

Bilgisayarlar belirli durumlarda eş zamanlı çalışma yerine, işlemleri belirli sırada yürütmektedirler. Bir işlemin başlaması diğer bir işlemin sonucuna göre belirlenmektedir. Bu çalışma esasına eşzamansız çalışma adı verilir.

Bellekte bekleyen veriler üzerinde değişiklik yapılmasına dayanan saldırı biçimine eşzamanız saldırı denmektedir. Örneğin herhangi bir programla yapılan çalışmanın sonuçlarını yazıcıdan almak için diğer işlemlerin bitmesinin beklendiği esnada, iyi programlama bilgisine sahip kişiler bellekte bekleyen bu veriler üzerinde istekleri doğrultusunda ekleme, silme veya değişiklik yapabilme imkânına sahiptirler.

2.18.18. İstem Dışı Alınan Elektronik İletiler

İstem dışı alınan elektronik postalar olan *"spam"* özellikle son yıllarda birçok kullanıcının, büyük bilişim sistemleri yönetici ve kullanıcılarının uğraştığı önemli bir sorun haline gelmiştir. Spamsözcüğü, ABD kaynaklı olup ilk defa Firma Hormel Foods Corporation'un ürettiği gıdalarla ilgili kullandığı bir kısaltmadır ve *"spiced pork and ham"* sözcüklerinin baş harflerinden oluşmaktadır. Bu kısaltma ilgisiz olmasına rağmen zamanla kitlelere istem dışı gönderilen elektronik postalar için kullanılmaya başlanmıştır. Uluslararası Ticaret Örgütü'nün 1996 yılında yayınlamış olduğu "ICC Guidelinies on Interactive Marketing Communicating"de spam, bir bülten veya

2 Dülger s.105.

3 Dülger s.110.

haber grubu üzerinden ticari amaç taşımayan, bu forum konuları ile ilgili olmayan ve gönderilmesine açıkça izin verilmeyen reklam olarak tanımlanmaktadır.

Spam, genellikle bir ürünün reklamı, pazarlanması ve pornografik içerikli reklam ve mesajların dünya çapında kitlelere ulaştırılması amacıyla kullanılmaktadır. Bu tür mesajların, bünyesinde çok sayıda elektronik posta adresini barındıran kuruluşların sahip oldukları veri tabanlarını satmalarıyla arttığı belirtilmektedir.[4]

2.18.19. DNS'in Haksız Şekilde Kötüye Kullanılması

Yaygın olarak görülen suçlardan birisi de web sayfası hırsızlığıdır. Bir web sitesine alan adı verilen adreslerden ulaşılır. Alan adları sunucuları (DNS) veri tabanında tutulur ve tüm dünyaya ilan edilir. Bir internet kullanıcısı web sitesine ulaşmak istediğinde, web tarayıcısı alan adının DNS sorgulamasını yaparak web sayfasının bulunduğu sunucunun IP adresini öğrenmekte ve bu IP adresinden sayfayı getirmektedir.

Bir kişi web sayfası yayınlamak istediğinde önce bir alan adı almak zorundadır. Bunun için alan adı hizmeti veren servis sağlayıcılara müracaat eder. Eğer bu müracaattan önce, bir kişi daha hızlı davranıp alan adını tescil ettirirse, isim hakkı o kişinin olur. Tescil edilmiş alan adları da hackerlar veya bu bilgiye erişebilen bir internet servis sağlayıcı (İSS) çalışanı tarafından kendileri veya üçüncü bir kişi lehine olacak şekilde tescil kaydını değiştirebilirler.

Bu şahıslar daha sonra tescil ettirdikleri alan adlarını yüksek ücretlerle olması gereken gerçek sahiplerine satmaya çalışmaktadırlar.

Bu suç internet servis sağlayıcılarının herhangi bir şekilde internet başvurusuna ait bilgileri kötü niyetli üçüncü kişilere sızdırması şeklinde işlenebilir. Aynı zamanda servis sağlayıcısının sistemlerine bilgisayar korsanlarının girerek bilgilere erişmesi şeklinde de işlenebilir.

2.18.20. Web Sayfası Yönlendirme

Web sayfası yönlendirme, internet sitelerinin alan adları ile IP adreslerinin tutulduğu veri tabanları olan DNS sunucularda hukuka aykırı olarak değişiklik yapılarak web sitesinin bir başka IP adresine yönlendirilmesidir.

Kullanıcılar siteye ulaşmak için alan adını web tarayıcısına girerler. Ancak DNS kayıtları değiştirildiği için kullanıcı gitmesi gereken IP adresi yerine, faillerin istedikleri adrese yönlendirilir ve bambaşka bir siteye ulaşır.

Bu yöntem genellikle banka web sayfasına ulaşmak isteyen kullanıcılara uygulanmaktadır. Kullanıcıların yönlendirildiği web sayfası, gerçekte gidilmek istenen web sayfasına benzer şekilde tasarlanmış başka bir web sayfasıdır. Kullanıcı bu sayfa üzerinde şifrelerini girdiğinde, bilgisayar korsanı bu şifreleri elde etmektedir. Özellikle internet üzerinden alışveriş ve bankacılık işlemlerinin yaygınlaşması, suçluların bu yöntemi kullanarak banka kredi kartları bilgilerini temin edebilme eğilimlerini artırmıştır.

4 Dülger, s.113.

2.18.21. Sırtlama

Sırtlama, fiziksel ya da elektronik yollar aracılığıyla bilişim sistemlerine yetkisiz olarak girme tekniğidir.

Fiziksel sırtlama, bilişim sistemlerinin yetki ile erişilen kısımlarına, girişe yetkili olan bir kullanıcının giriş yetkisinin kullanılarak girilmesidir.

Elektronik sırtlama ise, bilişim sistemlerine bağlı kullanıcıların bağlandıkları hatlar kullanılarak bilişim sistemlerine yetkisiz olarak erişilmesidir.

2.18.22. Mantık Bombaları

Mantık bombası aslında truva atı yazılımlarının bir türüdür. Aynen truva atı gibi bilişim sistemine yararlı bir yazılımgörüntüsünde sisteme girmekte ve sistem içinde normal şekilde çalışıp hiçbir zarar verici işlemde bulunmamaktadır. Ancak yazılımın içinde belirlenmiş özel durumların gerçekleşmesi ya da yazılım tarafından belirtilen bir tarihin gelmesi halinde gerçek kimliğine bürünerek hareket etmekte ve zarar verici işlemlerine başlamaktadır.[5]

Mantık bombası yazılımları tamamen içine girdiği bilişim sistemine zarar vermek amacıyla oluşturuldukları için harekete geçtiklerinde sistem için yıkıcı olmaktadırlar. Ülkemizde 26.4.1999 tarihinde ortaya çıkan "Çernobil virüsü olayı" mantık bombaları için iyi bir örnektir. CIH adlı virüs kendisini yazan kişi tarafından yerel bir bilişim konferansında yazılımı yararlı olarak tanıtıp çeşitli ülkelerden gelen katılımcılara dağıtmıştır. Bu kişiler tarafından yazılım çok kısa sürede Avusturya, Avustralya, İsrail, Şili, İsviçre, İsveç, ABD, Rusya ve İngiltere gibi ülkelere ulaştırılmıştır. Windows 95 ve Windows 98 işletim yazılımlarında çalışan mantık bombası kendisini ihtiva eden bir kurulum dosyası çalıştırıldığında etkin hale gelmekte ve bilişim sisteminin hafızasında beklemektedir. Yazılımher ayın 26'sında zarar verici eylemlerine başlamakta ve sisteme onarılamazölçüde zararlar vermektedir. Bu yazılım ülkemizde de çok sayıda bilişim sistemine zarar vermiş ve önemli ölçüde maddî kayba yol açmıştır.[6]

2.18.23. Yerine Geçme

Belli bir ağa bağlı olan bilişim sistemleri, erişim yetkileri yönünden bölümlere ayrılırlar. Sistemlere erişim imkânı her bilgisayar için eşit düzeyde olmayabilir.
Sistem kullanıcıları farklı seviyelerde yetkilendirilmektedir. Kullanıcılar, sahip oldukları kullanıcı isim ve şifreleri sayesinde bilişim sistemlerinde farklı seviyelerde işlem yapabilmektedirler.

Gelişen teknoloji ile birlikte, kullanıcı isim ve şifrelerinin yanında parmak izi, göz retina yapısı gibi kişisel özellikler de sistem erişimlerinde kullanılmaya başlamıştır. Bilişim sistemlerine erişim yetkisi olan bir kişinin başkaları tarafından, kullanıcı isim ve şifresinin yazılarak veya kişisel özelliklerinin taklit edilerek sistemlere giriş yapılmasına yerine geçme denmektedir.

2.18.24. Bukalemun

5 Dülger, s.112.
6 Dülger, s.112.

Bukalemun adlı yazılımlar truva atı yazılımı gibi sistemi aldatma yoluyla içeri girerler. Sistem için normal çalışan, zararsız bir yazılım gibi davranan ve onun niteliklerine sahipmiş gibi görünen bukalemunlar, sistemin içine girdikten sonra gerçek kimliklerini ortaya çıkartmakta ve zarar verici eylemlerine başlamaktadırlar. Bu yazılım kendisini saklamaktaki başarısı nedeniyle bu adı almıştır.

Bukalemun yazılımları, özellikle çok kullanıcılı sistemlerde içine girdikleri bilişim sisteminde bulunan kullanıcı adlarını ve şifrelerini, verileri taklit edebilme özelliği sayesinde gizli bir dosyaya kaydeder ve bundan sonra sistemin monitöründe "sistemin bakım için geçici bir süre kapatılacağı" uyarısını verir. Sistem kapandıktan sonra bukalemun yazılımını kullanan kişi içine girdiği sistemde istediği yere ulaşabilir ve eylemlerini gerçekleştirebilir.[7]

2.18.25. Hukuka Aykırı İçerik Sağlama

Bilişim suçlarının çok sık karşılaşılan diğer bir işlenme şekli de hukuka aykırı içeriklerin bilişim sistemlerinde bulundurularak veri iletim ağları sayesinde diğer kullanıcıların erişimine sunulmasıdır. Bu içerikler ırkçı, ayrımcı, şiddeti teşvik eden ya da kişilik haklarına tecavüz eden içerikler olabileceği gibi insan ticareti ya da çocuk pornografisi ile ilgili içerikler de olabilmektedir.

Ülkemizde yaşanan bir olayda, üniversitede idari görevleri de bulunan bir öğretim üyesine, kendisinin üniversitedeki tutum ve uygulamalarına yönelik olarak hakaretve tehditler içeren bir elektronik posta gönderilmiştir. Söz konusu postada, öğretim üyesinin Ankara'da bulunan bir yakınının takip edildiği ve kendisinin hareketlerini düzeltmemesi halinde yakınına zarar verileceği tehdidi bulunmaktadır. Bu elektronik posta üzerinde yapılan teknik çalışmalar sonucunda öncelikle iletinin Türkiye içinden gönderildiği, sonra da öğretim üyesinin bulunduğu aynı ilden gönderildiği tespit edilmiştir. Elektronik izler takip edilmek suretiyle sonunda bu eylemi gerçekleştiren fail yakalanmış ve mahkemeye sevk edilmiştir.[8]

2.19. DNS (Domain Name System - Alan Adı Sistemi)

İnternet uzayını bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan bir sistemdir.

2.20. Sunucu

Bilgisayar ağlarında diğer ağ bileşenlerinin (kullanıcıların) erişebileceği, kullanımına ve/veya paylaşımına açık kaynakları barındıran bir bilgisayar birimidir.

2.21. Internet Ortamı

Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan İnternet üzerinde oluşturulan ortamdır.

7 Dülger s.111.

8 Dülger s.115.

2.22. Internet Ortamında Yapılan Yayın

İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verilerdir.

2.23. Erişim

Herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılmasıdır.

2.24. İlgi

Verilerin anlam kazanmış biçimidir.

2.25. Cracker

Ücretli programları kırarak (crack) ücretsiz kullanılmasını sağlayan kişilerdir. Hacker ile Cracker birbirine karıştırılmamalıdır. Cracker programları kırmaz, yalnızca program üzerinde ayarlandığı gibi değişiklikler yaparak ücretsiz kullanım, tema, dil gibi değişiklikleri program üzerine kurarlar. Türkçede 'crack' yerine 'ilaç' sözcüğü de kullanılmaktadır.

Crack, program kırma eylemine ve ters mühendisliğe verilen isimdir. Hack ise, kelime anlamı olarak "küçük parçalar koparmak" anlamındadır ve hacker'lerin algoritmik düşünme, nesnel bir topoloji oluşturma, istatistik (makul aralıklar içinde iterasyon yapma ve uyumu (korelasyon) yorumlama) yetenekleri tesadüfi gelişmiştir. Düşük seviye programlama donanım üzerinde sağlam geçmişleri ve iddiaları yoktur.

2.26. Hacker

Hacker, diğer adıyla bilgisayar korsanı olarak bilinir. Şahsî bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişilerdir. Bilgisayar programcılığı alanında, bir hacker bir exploit'e bir dizi düzeltme uygulama ya da varolan kodları kullanma yoluyla bir amaca ulaşan ya da onu 'kıran' bir programcıdır. Bilişim sistemleri üzerinde, başka sistemlere veya web sitelerine farklı yöntemlerle zarar verirler.

TÜRK CEZA KANUNU'NDA DÜZENLENEN BİLİŞİM SUÇLARI

3.1. Bilişim Alanında İşlenen Suçlar
3.1.1. Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Sistemde Kalma Suçu (TCK m.243)
3.2.1. Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması Suçu ile Verilerin Yok Edilmesi veya Değiştirilmesi Suçu (TCK m.244/1–2)
3.1.3. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçları (m.245)
3.2. Bilişim Sisteminin Kullanılmasının Suçun Nitelikli Hâli Olarak Düzenlendiği Suçlar
3.2.1. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Hırsızlık Suçu (TCK m.142/2 -e)
3.2.2. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Dolandırıcılık Suçu (m.158/1 -f)
3.3. Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Suçlar
3.3.1. Ödeme Sistemleri BKK 23, 39, Banka Kartları ve Kredi Kartları Kanununda Düzenlenen
3.3.2. Elektronik İmza Kanunu'nda Yer Alan Suçlar (EİK m. 16-17)
3.3.3. Online Kumar (TCK 228)
3.3.4. Çocuk Pornografisi (TCK 226/3)
3.3.5. Haberleşmenin Engellenmesi (TCK 124)
3.3.6. Özel Hayata ve Hayatın Gizli Alanına Karşı İşlenen Suçlar/Kişisel Verilere Karşı Suçlar (TCK 132,133,134,135,136,137,138)
3.3.6.1. Haberleşmenin Gizliliğini İhlal Suçu (m.132)
3.3.6.2. Kişiler Arasındaki Konuşmaların Dinlenmesi veya Kayda Alınması Suçu m.133)
3.3.6.3. Özel Hayatın Gizliliğini İhlal Suçu (m.134)
3.3.6.4. Kişisel Verilerin Kaydedilmesi
3.3.6.5. Kişisel Verileri Verme veya Ele Geçirme Suçu (m.136)
3.3.6.6. Verilerin Yok Edilmemesi Suçu (TCK m.138)
3.3.7. DEVLET SIRLARINA KARŞI SUÇLAR (TCK 326/1, 327,329, 330, 333, 334, 335, 336, 337) Fikir ve Sanat Eserleri Kanunu Madde 71
3.3.7. TCK 125, 106, 105, 267, 107, 148
3.3.8. Sanal Oyun Karakterinin ve Araçlarının Çalınması

Bilişim Alanında Suçlar	• Hukukar aykırı olarak bilişim sistemine girme suçu (m.243) • Bilişim sisteminin işleyişinin engellenmesi,bozulması, verilerin yok edilmesi veya değiştirilmesi (m. 244/1-2) • Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m.244/4) • Banka veya kredi kartlarının kötüye kullanılması suçu (m.245)
Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar	• Kişisel verilerin kaydedilmesi suçu (m. 135) • Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu (m.136) • Verilerin yok edilmesi suçu (m.138)
TCK'nin Çeşitli Bölümlerinde Bilişim Sistemleriyle İşlenmesi Olanaklı Suçlar	• Haberleşmenin gizliliğinin ihlali suçu (m. 132) • Hakaret (m. 125) • Haberleşmenin engellenmesi suçu (m. 124 • Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (m. 142/2-e) • Bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu (m.158/1-f)

3. TÜRK CEZA KANUNU'NDA DÜZENLENEN BİLİŞİM SUÇLARI

3.1. Bilişim Alanında İşlenen Suçlar

3.1.1. Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Sistemde Kalma Suçu (TCK m.243)

"Madde 243

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

*(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.***"**

a. Korunan Hukuksal Değer

Bu suçla korunan hukuksal değerbilişim sisteminin güvenliğidir. Bilişim sistemine hukuka aykırı erişimin engellenmesiyle sistemin malikî ya da kullanıcısı gibi bir şekilde sistemden faydalanan kişilerin çok sayıdaki farklı türden çıkarları koruma altına alınmaktadır. Bu kişilerin çıkarları; verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı ya da kişilerin ya da kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuksal değerler olabilmektedir. Ancak tüm bunların üstünde ve bunları

kapsayacak şekilde yer alan hukuksal değer bilişim sisteminin güvenliğidir.[1]

b. Tipikliğin Maddî Unsurları

aa.Fail: Madde metninde suçu işleyecek kişi açısından "kimse" sözcüğü kullanılarak herhangi bir özellik belirtilmemiştir; bu nedenle bu suçun faili herkes olabilir. Dolayısıyla hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu fail açısından bir özellik göstermemektedir.[2]

bb.Mağdur: Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu mağdur açısından bir özellik göstermemektedir, herkes bu suçun mağduru olabilir. Mağdur, belirli bir suçla zarara veya tehlikeye uğratılan hak veya çıkarın, suçla korunan hukuksal değerin sahibi olan kişidir. Bu suçun işlenmesiyle de bilişim sisteminin güvenliğinin ihlal edilmesiyle çıkarı zarara uğratılan kişi suçun mağduru olmaktadır. Bize göre ancak gerçek kişiler suçun mağduru olabilir, tüzel kişiler ancak suçtan zarar gören olabilirler, dolayısıyla bu suçun mağduru da gerçek kişilerdir, ancak bir şirketin ya da kamu tüzel kişisinin sistemine karşı bu suç işlendiğinde söz konusu tüzel kişiler suçtan zarar gören olacaklardır. [3]

cc.Suçun Konusu: Suçun konusunu, hukuka aykırı olarak içine girilen veya orada kalmaya devam edilen "bilişimsistemi" oluşturmaktadır. Ancak, 1. fıkra açısından suçun konusunu sistemin kendisi oluştururken, 2. fıkrada yer alan suçun nitelikli hali için suçun konusu "bedeli karşılığı yararlanabilinen bir bilişim sistemi", 3. fıkrada yer alan suçun neticesi sebebiyle ağırlaşmış hali için ise "bilişim sisteminde yer alan veriler" suçun konusunu oluşturmaktadır.[4]

dd.Eylem: Hukuka aykırı olarak bilişimsistemine girme ve sistemde kalma suçunun maddî unsurunu, hangi yolla olursa olsun bir bilişim sistemine girilmesi ve bilişim sisteminde kalmaya devam edilmesi hareketleri oluşturmaktadır. Bu, 243. maddede "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden" şeklindeki yer ifadeden, açıkça anlaşılmaktadır.

"Giren" ibaresinin "erişim" şeklinde düzeltilmesi gerekmektedir. Nitekim uygulamada, "giren" ibaresi "erişim" şeklinde anlaşılmaktadır.

Kanun ibaresinde yer alan "giren ve orada kalmaya devam eden" şeklindeki düzenlenmesi nedeniyle failin, girme ve orada kalmaya devam etme eylemini birlikte gerçekleştirmesi gerekmektedir. Ancak bu düzenleme yerinde değildir. Yalnızca "girmek"eylemi bu fiilin oluşumu bakımından yeterlidir. Ayrıca orada kalmayı aramak maddenin uygulanmasını veya korunan hukukî yararı imkânsız hâle getirmektedir. Maddenin gerekçesinde, "Bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiilini suç haline getirmiştir." denmiştir. Kanunilik ilkesi bakımından maddedeki düzenlemeyi bu şekilde anlamak mümkün değildir. Burada "giren ve orada kalmaya devam eden" ibaresinin "giren veya orada kalmaya devam eden" şeklinde değişiklik yapılması yerinde olacaktır. Bununla birlikte, Avrupa Siber Suçlar Sözleşmesi'ne uygun olarak, "giren ve orada kalmaya devam eden" ayrımı yerine "erişim" ibaresinin getirilmesi de yerinde olacaktır.

1 Dülger, s.316.
2 Dülger, s.323.
3 Dülger, s.332.
4 Dülger, s.333.

Bilişim sistemine girme ve sistemde kalma suçunun oluşması için bilişimsistemine girilmesi ve orada kalınması hareketlerinin yapılması yeterli görülmekte, suçun gerçekleşmesi için ayrıca bir zararın oluşması ya da zararın doğması için yakın bir tehlikenin oluşması gerekmemektedir. Bu nedenle bu bir soyut tehlike suçudur.[5]

ee. Nitelikli Haller TCK 243. maddesinin 2. fıkrasında, hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma eylemlerinin, "bedeli karşılığı yararlanılabilen sistemler" hakkında işlenmesi yasa koyucu tarafından cezayı hafifletici bir neden olarak öngörülmüştür.[6]

c. Tipikliğin Manevi Unsurları

Bilişim sistemine girme ve sistemde kalmaya devam etme suçunun manevi unsurunu kast oluşturmaktadır, yasada açıkça suçun taksirle işlenebileceği belirtilmediği için suçun taksirle işlenmesi mümkün değildir.[7]

d. Hukuka Aykırılık Unsuru

5237 sayılı TCK'da hukuka uygunluk nedenleri dört ana grupta toplanmıştır. Bunlar, "hakkın kullanılması" (m.26/1), "kanunun hükmünü yerine getirme" (m.24/1), "meşru savunma" (m.25/1) ve "ilgilinin rızası" (m.26/2) halleridir. Bilişimsistemine girme ve sistemde kalmaya devam etme suçu açısından söz konusu olabilecek hukuka uygunluk nedenleri,"kanunun hükmünü yerine getirme" ve "ilgilinin rızası"dır. [8]

e. Suçun Özel Görünüş Biçimleri

aa.Teşebbüs: Bilişimsistemine girme ve sistemde kalma suçunda maddî unsur olarak sisteme girme ve orada kalmaya devam etme eylemlerinin gerçekleştirilmesi öngörülmüş, bunun dışında bir zararın meydana gelmesi suçun oluşumu için aranmamıştır. Söz konusu suç tipi bu özelliğiyle neticesiz bir suç tipidir. Hareketle netice arasında bir ayrım olmadığı için, hareketin tamamlanması ancak neticenin failin elinde olmayan bir nedenle gerçekleşmemesi halinde suça teşebbüsün gerçekleşmesi mümkün değildir.Zîra hareketin yapılmasıyla suç tamamlanmış olacaktır. Bilişim sistemine girildikten sonra sistemde kalma fiilinin teşebbüs aşamasında kalıp kalamayacağı doktrinde tartışılsa da bu suçun teşebbüse elverişli olmadığı görüşü baskındır.[9]

bb.İştirak: Bu suça iştirak TCK'nın iştirak hükümleri gereği her zaman mümkündür.[10]

cc.İçtima: İnceleme konusu suç açısından akla gelen ilk durum zincirleme suçun oluşup oluşmayacağıdır. Gerçekten de failin aynı suç işleme kararıyla bir bilişim sistemine farklı zaman dilimlerinde girmesi ve sistemde kalmaya devam etmesi mümkündür. İşte bu durumda TCK'nın 43. maddesinin uygulanıp uygulanamayacağının

5 Dülger, s.334.
6 Dülger, s.344.
7 Dülger, s.351.
8 Dülger, s.355.
9 Dülger, s.370.
10 Dülger, s.372.

belirlenmesi gerekmektedir. Örneğin bir bilişim korsanıaynı bilişim sistemine çok kısa aralıklarla defalarca girip çıkıyor ve sistemde belli bir süre kalıyor, böylelikle de sistem kullanıcılarına bu işi yapabildiğini ispata çalışıyorsa ya da belli bir bilgiyi öğrenmek için hattın kopması nedeniyle ardı ardına giriş yapıyor, kısa da olsa sistemde kalıp istediği bilgiyi elde edemeden sistemden dışarı çıkmak zorunda kalıyorsa bu durumda zincirleme suç uygulanacak mıdır? Bize göre bu durumda faile TCK'nın 43. maddesinin uygulanması ve tek suçtan dolayı cezasının arttırılarak verilmesi gerekir. Eğer fail aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla sisteme giriyor ve orada kalmaya devam ediyorsa artık burada failin aynı suç işleme kararıyla hareket ettiği söylenemeyecek ve her eylem için ayrı ceza verilip cezaların içtimaıkuralı uygulanacaktır.[11]

f. Yaptırım, Soruşturma ve Kovuşturma

Bilişim sistemine girme ve sistemde kalma suçunu işleyen failler için "bir yıla kadar hapis veya Adlî para cezası" öngörülmüştür. Cezalar seçimlik olarak düzenlendiği için iki cezanın birlikte verilmesi mümkün değildir; fail hakkında ya hürriyeti bağlayıcı ceza ya da Adlî para cezasına karar verilecektir.

Adlî para cezasının miktarı ve hesaplanma yöntemi TCK'nın 52. maddesinde gösterilmiştir.

Bu suç açısından 2. fıkrada belirtilen cezayı hafifletici nitelikli halin gerçekleşmesi halinde yukarıda belirtilen cezalar yarı oranına kadar indirilecektir.

243. maddenin 3. fıkrasında belirtilen suçun netice sebebiyle ağırlaşan halinin gerçekleşmesi halinde ise faile verilecek ceza altı aydan iki yıla kadar hapis cezası olacak ve bu durumda faile hürriyeti bağlayıcı ceza yerine Adlî para cezası verilemeyecektir.[12]

"Sanığın Kalley Internet Cafe'nin sahibi olduğu, iş yerindeki 70 adet bilgisayarın gözetimi ve denetimi için gerekli hassasiyeti göstermemesi sebebiyle kusurlu olduğu gerekçesiyle cezalandırılmasına karar verilmiş ise de, adı geçen iş yerindeki IP numarası 81.215.188.170 olan bilgisayardan müştekinin elektronik posta adresine girilmesinden sanığın sorumluluğu olmamasına rağmen, üzerine atılı suçtan beraatine dair karar verilmesi gerekirken yazılı şekilde cezalandırılmasında..." 11. CD., Kt. 14.5.2010, E. 2009/23397, K. 2010/6054."

3.1.2. Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması Suçu ile Verilerin Yok Edilmesi veya Değiştirilmesi Suçu (TCK m.244/1-2)

"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında

11 Dülger, s.373.

12 Dülger, s.377.

artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

a. Korunan Hukuksal Değer

244. maddenin 1. ve 2. fıkrasında düzenlenen suçlarla paralel olan ASSS'nin 4. ve 5. maddelerine ilişkin açıklayıcı raporda, 4. maddede korunan hukuksal değerin bilişimsisteminde yer alan verilere veya yazılımlara zarar verilmesini, veri ve yazılımların bozulmasını, zarar görmesini engellemek, böylelikle bunların doğru ve işlevsel olarak çalışmalarını sağlamak olduğu ifade edilmektedir. ASSS'nin 5. maddesinde korunan hukuksal değerin ise temel olarak bilişim sistemlerine karşı gerçekleştirilen saldırıların önlenmesi, bilişim sistemlerinin sağlıklı şekilde kullanımının sağlanması ve buna yönelecek haksız davranışlara engel olunması olduğu belirtilmektedir. Böylelikle bilişim sistemi kullanıcılarının bu sistemleri işlevsel bir şekilde kullanmaya yönelik hakları korunmaktadır.Buna göre yukarıda da belirttiğimiz üzere sistemlerin ve verilerin sağlam ve sağlıklı bir şekilde çalışabilirliği korunmaktadır.[13]

244/4'teki suçun yasa maddesindeki tanımına göre, failin bilişim sistemiaracılığıyla gerçekleştirdiği eylemler neticesinde suçun oluşması için failin hukuka aykırı bir yarar elde etmesi gerekmektedir; ancak bunun nasıl bir yarar olduğu açıklanmamıştır. Yararın türü bakımından bir ayrım yapılmadığına göre fail tarafından elde edilen maddî ya da manevî yarar suçla korunan hukuksal değeri oluşturmaktadır.

b. Tipikliğin Maddî Unsurları

aa.Fail: Herkes bu suçların faili olabilir, yasa maddesinde bu açıdan bir özellik belirtilmemiştir. Bu suçlar ile hem bir bütün hâlinde bilişim sistemine hem de verilere zarar verilmesi eylemleri suç olarak düzenlenmektedir. Bu nedenle kişinin, başkasının haklarına zarar vermeksizin herhangi bir bilişim sisteminde bulunan kendisine ait verilere zarar vermesi suç oluşturmayacağından failin tespit edilmesi önem taşımaktadır. Ancak failin kendisine ait olmayan bir bilişim sisteminde bulunan kendisine ait olan verileri yok etmek ya da erişilmez kılmak için sistemin işleyişini bozması ya da engel olması halinde ise her ne kadar 244. maddenin 2. fıkrasındaki suç gerçekleşmeyecek olsa da 1. fıkradaki suç gerçekleşmiş olacaktır.[14]

244. maddenin 4. fıkrasındaki suçta da fail herkes olabilir.

bb.Mağdur: Bilişimsisteminin işleyişinin engellenmesi ve bozulması suçu ile verilerin yok edilmesi veya değiştirilmesi suçunda herkes suçun mağduru olabilir, suç tipleri bu açıdan bir özellik göstermemektedir. Yukarıda suçlarla korunan hukuksal değerler ve fail konularında yapılan açıklamalar ışığında ifade edilmelidir ki bu suçların mağduru olmak için mutlaka bilişim sisteminin ya da zarara uğrayan verilerin maliki veya zilyedi olunması gerekmemektedir.

Bu suçları oluşturan hareketlerin gerçekleştirilmesi sonucunda; bilişimsistemine ve/veya verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel

13 Dülger, s.381.

14 Dülger, s.384.

çalışma, bilgi vb. değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşılmasında ve kullanılmasında çıkarı bulunan ve bilişim sistemi ve/veya veriler üzerinde tasarruf yetkisi bulunan kişi bu suçun mağduru olacaktır.
Bilişimsistemi aracılığıyla hukuka aykırı yarar sağlamak suçunda mağdur açısından her hangi bir özellik aranmamıştır. Mağdur herkes olabilir.[15]

cc.Suçların Konusu: 244. maddenin 2. fıkrasında düzenlenen suçu, 1. fıkrada düzenlenen suçtan ayıran en önemli husus suçun konusudur. 1. fıkrada düzenlenen suçun konusunu bilişim sistemi oluştururken, 2. fıkrada yer alan suçun konusunu bilişim sisteminde yer alan veriler oluşturmaktadır.

244. maddenin 4. fıkrasında düzenlenen suçun konusunu failin sağladığı "hukuka aykırı yarar" oluşturmaktadır. Bu yarar ekonomik değeri olan mali bir yarar olabileceği gibi ekonomik birgetirisi ve değeri olmayan tamamen duyguları tatmine yönelik manevi bir yarar da olabilecektir.[16]

dd. Eylemler:

aaa. Bilişim Sisteminin İşleyişini Engellemek (TCK m. 244/1): Bu ifadeyle yasa koyucunun belirttiği hareket, sisteme etkide bulunularak sistemin düzgün işlemesinden elde edilecek her türlü faydanın engellenmesi ve sistemin işlevlerini yerine getirememesidir. Yasa koyucu burada kavramı çok geniş tutmuş ve nasıl olduğunu aramaksızın sistemin işleyişini bozmak dışında sistemin işlemesini engelleyen her türlü eylemi buraya dâhil etmek istemiştir.[17]

bbb. Bilişim Sisteminin İşleyişini Bozmak (TCK m. 244/1): Bozmak sözcüğünün anlamı TDK'nın sözlüğünde "bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek; bir yerin, bir şeyin düzenini karıştırmak; dokunmak, zarar vermek; kötü duruma getirmek" olarak açıklanmaktadır. Bu açıklamadan hareketle, 244. maddenin 1. fıkrasında yer alan bozmak ifadesiyle bilişim sisteminin kendisinden beklenilen işi yapamayacak duruma getirilmesi, bilişim sisteminin düzeninin karıştırılması, bilişim sistemine zarar verilmesi veya kötü duruma getirilmesi kastedilmektedir. Bir başka deyişle bilişim sisteminin işleyişinin bozulması, sistemin kısmen ya da tamamen işleyemez hale getirilmesidir.[18]

ccc. Verileri Bozmak (TCK m. 244/2): Yukarıda bilişim sisteminin işleyişini bozmak hareketi açısından anlatılanlar, verileri bozmak hareketi açısından da geçerlidir. Zaten bilişim sistemine verilen fizikî zararların dışında kalan hemen tüm zarar verici eylemler verilerle olmakta ve verilere zarar verme hareketini oluşturmaktadır.
Bilişim sisteminin işleyişinin engellenmesi için verilerin bozulması hâlinde failin amacı sistemde bulunan verilere zarar vermek değil bir şekilde bilişim sisteminin işleyişini bozmaktır; oysaki maddenin 2. fıkrasında yer alan verileri bozmak hareketinde fail bilişim sisteminin işleyişine zarar vermek istememekte bilişim sisteminin içerdiği bir kısım verileri örneğin bir uygulama yazılımını ya da depolanmış bazı bilgileri kullanılamaz hale getirmek istemektedir. Ancak yukarıda da belirttiğimiz üzere faildeki bu amaç suç tipi açısından bir unsur olmayıp somut eyleme hangi fıkranın uygulanacağının belirlenmesi açısından bir yorum aracı olabilir. Yoksa her iki fıkradaki

15 Dülger, s.384.
16 Dülger, s.385.
17 Dülger, s.387.
18 Dülger, s.388.

suçun oluşumu açısından failin kastının varlığı yeterlidir.[19]

ddd. Verileri Yok Etmek (TCK m. 244/2): Yok etmek sözcüğünün anlamı TDK'nın sözlüğünde "varlığına son vermek, ortadan kaldırmak, ifna etmek, izale etmek" olarak açıklanmaktadır. Ancak bilişim sistemlerinde yer alan veriler açısından yukarıda açıklanan gerçek anlamında olduğu gibi verileri tamamen ortadan kaldırmak ya da varlığına son vermek her durumda mümkün değildir. Bu nedenle yasa koyucucunun bu ifadeyle somut anlamda yok etmek eylemini değil, bilişim alanında geçerli olan soyut anlamda mantıksal yok etmek eylemini kastettiği belirtilmelidir.[20]

eee. Verileri Değiştirmek (TCK m. 244/2): Verilerin değiştirilmesi eylemiyle, bir veri ya da veri grubu yerine başka verilerin konulması kastedilmektedir. Bu birkaç veriden oluşan bir bilgi notu ya da resmin değiştirilmesi şeklinde olabileceği gibi verilerden oluşan örneğin bir uygulama yazılımının değiştirilmesi şeklinde de olabilecektir. Örneğin kullanıcının sisteme koyduğu şifrenin yerine bir başka şifrenin konulması halinde bu durum söz konusu olacaktır.[21]

fff. Verileri Erişilmez Kılmak (TCK m. 244/2): Verilerin erişilmez kılınması, verilerin malikinin ya da ilgilisinin istediği zaman ve istediği verilere ulaşmasının engellenmesi anlamına gelmektedir. Bu hareket neticesinde veribütünlüğü korunmaktadır, veri yok edilmemiş ya da bozulmamıştır, ancak verilere ulaşım bir şekilde engellenmiştir ve veri üzerindeki hak sahibi kendi verilerine erişememektedir. Bu sonuç virus bulaştırmak, şifrekoymak vs. gibi çok çeşitli şekillerde sağlanabilir.[22]

ggg. Bilişim Sistemine Veri Yerleştirmek (TCK m. 244/2): Bilişim sistemine veri yerleştirmek hareketiyle, fail tarafından bilişim sistemine ya da veri taşıma aracına dışarıdan ve sistemin malikî ya da ilgilisinden izin alınmaksızın çeşitli verilerin sisteme kaydedilmesi, yüklenilmesi ya da eklenilmesi kast edilmektedir. Bu yerleştirme hareketi, bilgisayarın başına oturup "harici bellek" ya da "USB" gibi veritaşıma aracını sürücü donanıma yerleştirip içindeki verileri bilgisayara yüklemek şeklinde yapılabileceği gibi, internet üzerinden veri yüklemek şeklinde de gerçekleştirilebilecektir. [23]

hhh. Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Göndermek (TCK m. 244/2): Bununla, bilişim sisteminde bulunan verilerin bilişim sistemi dışında bulunan bir başka bilişim sistemine ya da veri taşıma aracına aktarılması, kaydedilmesi ya da kopyalanması hareketleri belirtilmektedir.Bilişim sisteminde var olan verilerin başka yere gönderilmesi eylemi veri iletim ağları üzerinden örneğin internet ya da "wifi" ile bir başka bilişim sistemine verilerin aktarılması yoluyla gerçekleştirilebileceği gibi, verilerin bulunduğu bilgisayara bir veri taşıma aracının bağlanması ve verilerin bu aracın üzerine kaydedilmesi yoluyla da yapılabilecektir.[24]

19 Dülger, s.389.
20 Dülger, s.390.
21 Dülger, s.391.
22 Dülger, s.391.
23 Dülger, s.392.
24 Dülger, s.398.

"Sanığın, katılan M. Ç.'nin MSN şifresini kırıp değiştirerek sözkonusu bilişim sistemine katılanın kendi şifresi ile girişini erişilmez kıldığı anlaşılmakla, CMK'nun 217. maddesi uyarınca duruşmadan edindiği kanaate göre delilleri değerlendirip vicdani kanıya ulaşan mahkemenin eylemin 5237 sayılı TCK.nun 244/2 maddesinde tarif edilen suçu oluşturduğu yönündeki sonucu itibariyle doğru olan kararında bir isabetsizlik görülmediğinden tebliğnamedeki iki nolu bozma düşüncesine iştirak olunmamıştır." 11. CD., Kt. 10.12.2012, E. 2010/9658, K. 2012/21340.

ıii. TCK m. 244/4'teki eylem: Bu suç tipi 244. maddenin 4. fıkrasından aynı maddenin 1. ve 2. fıkralarına yapılan atıfla düzenlendiği için; 244. maddenin 1. ve 2. fıkralarında düzenlenen bilişimsisteminin işleyişinin engellenmesi ve bozulması suçu ile verilerin yok edilmesi veya değiştirilmesi suçunun maddî unsurunu oluşturan eylemler, bu suçun da eylem unsurunu oluşturmaktadır. Buna göre bu suçun oluşabilmesi için failin bilişim sisteminin işleyişini engellemek, bilişim sistemin işleyişini bozmak, verileri bozmak, bilişim sistemine veri yerleştirmek, bilişim sisteminde var olan verileri başka bir yere göndermek, verileri erişilmez kılmak, verileri değiştirmek ve verileri yok etmek hareketlerinden birini ya da bir kaçını gerçekleştirmesi gerekmektedir. Dolayısıyla bu suç da seçimlik hareketli bir suç olarak düzenlenmiştir.

Yasa koyucu bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçunun gerçekleşmesi için failin gerçekleştirdiği eylemler neticesinde yasanın ifadesiyle "haksız bir çıkar sağlamasını" aramıştır. Haksız çıkar ifadesiyle kastedilen "hukuka aykırı yarardır". Bu yarar yukarıda da açıklandığı üzere mali haklara yönelik bir yarar olabileceği gibi manevi haklara yönelik bir yarar da olabilecektir. Bu durum her eylem açısından değerlendirilecektir. Failin gerçekleştirdiği eylemin sonucunda yarar elde edememesi durumunda bu suç oluşmayacaktır. Bu durumda 244/1–2 fıkralarında yer alan suçların gerçekleşmesi söz konusu olabilecektir.

ee. Suçun Nitelikli Hâli: TCK'nın 244. maddesinin 3. fıkrasında, her iki suç tipinde tanımlanan eylemlerin "bir banka veya kredikurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi" suçlarınnitelikli hâli olarak öngörülmüştür. Buna göre nitelikli halin gerçekleşmesi durumunda faile verilecek ceza yarı oranında arttırılacaktır.[25]

"Sanıkların O. bankası ATM'sinin çalışmasındaki aksaklığı fark ederek, çeşitli zamanlarda para çekme işlemi sırasında ATM'ye fizikî müdahalede bulunmak suretiyle cihazın para bloke edilmiş gibi işlem görmesini sağlayıp, çektikleri paranın hesaptan düşmesini engelleyerek menfaat elde ettiklerinin iddia ve kabul olunması karşısında eylemlerinin 765 sayılı TCK'nun 525/b-1 (5237 sayılı TCK'nun 244/4) maddesindeki "bilişim sistemini engellemek veya yanlış biçimde çalışmasını sağlamak suretiyle yarar sağlamak" suçuna uygun bulunduğu gözetilmeden yazılı şekilde 765 sayılı TCK'nun 525/b-2. maddesinden hüküm kurulmak suretiyle eksik ceza tayini..... bozmayı gerektirmiştir." 11. CD., Kt.

ff.Tipikliğin Manevî Unsuru: 244. maddenin 1. ve 2. fıkrasında yer alan her iki suçun da manevi unsurunu kast oluşturmaktadır. Ayrıca bu suçlarda failin belli bir saikle hareket etmesi aranmamaktadır. Ancak 2. fıkrada tanımlanan verilere ilişkin hareketlerin gerçekleştirilmesiyle sistemin işleyişinin engellenmesi veya bozulması da mümkündür. İşte böyle bir durumda failin eyleminin hangi fıkraya göre cezalandırılacağının belirlenmesinde suçun unsuru olarak belirtilmemişse de faildeki amacın yorum aracı olarak belirlenmesi gerekecektir. Suç tiplerinde açıkça

25 Dülger, s.398.

belirtilmediği için her iki suçun da taksirle işlenmesi mümkün değildir.[26]

d. Hukuka Aykırılık Unsuru

Suçla korunan hukuksal değer konusunda açıklandığı üzere bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile sistemin kesintisiz ve sağlıklı çalışması korunurken, verilerin yok edilmesi veya değiştirilmesi suçu ile veriler üzerinde tasarruf yetkisibulunan kişinin, verilere her hangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanmasındaki çıkarı korunmaktadır. Bu nedenle söz konusu bu hakların sahibinin ya da yetkilisinin rızası, hukuka uygunluk sebebi oluşturacaktır.[27]

e. Suçun Özel Görünüş Biçimleri

aa. Teşebbüs: Bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile verilerin yok edilmesi veya değiştirilmesi suçunun teşebbüs hâlinde kalması mümkündür. Bu, icra hareketlerine başlandıktan sonra bu hareketlerin yarıda kalması şeklinde olabileceği gibi suçun icrasına ilişkin bütün eylemler tamamlandıktan sonra suçun oluşumu için aranan netice meydana gelmeden failin elinde olmayan nedenlerle suçun gerçekleşmemesi şeklinde de olabilecektir.

TCK m. 244/4'te düzenlenen suç açısından teşebbüs özellik göstermektedir. Çünkü bu suç tipinin hareket unsuru 1. ve 2. fıkralarda düzenlenmiştir, suçun neticesi ise 4. fıkrada yer almaktadır. Failin kastının, gerçekleştirdiği eylemin neticesinde hukuka aykırı yarar elde etmek olduğunun tespit edilebildiği ancak 244. maddenin 1. ve 2. fıkralarında tanımlanan eylemin tamamlanıp neticenin failin elinde olmayan nedenlerle gerçekleşmediği durumda fail 244. maddenin 4. fıkrasına teşebbüsten dolayı cezalandırılmalıdır. Buna karşın failin kastının hukuka aykırı yarar elde etmek olduğunun ortaya konulamadığı ancak 1. veya 2. fıkradaki eylemlerin tamamlandığı durumlarda fail artık 4. fıkradaki suça teşebbüsten değil, 1. veya 2. fıkradaki suçun tamamlanmış hâlinden cezalandırılmalıdır.[28]

bb. İştirak: Suçlara iştirak açısından bir özellik söz konusu olmayıp TCK'nın 37., 38., 39. ve 40. maddelerindeki suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir.[29]

cc. İçtima: Bu suçların zincirleme şekilde işlenmesi mümkündür. Örneğin sistemin çalışmasının engellenmesi ya da hukuka aykırı olarak veri yerleştirilmesi için kısa zaman aralıklarıyla ve aynı suç işleme kararı çerçevesinde bilişim sistemine birçok kez etkide bulunulması hâlinde zincirleme suç gerçekleşecektir.

Ancak zincirleme suç bakımından varlığı gerekli olan aynı suçun işlenmesiyle kastedilen, yasanın aynı maddesinin birden çok kez ihlal edilmesi değildir. Çünkü TCK'nın birçok maddesinde birbirinden bağımsız suç tiplerine yer verilmektedir (örneğin TCK m. 132, 133, 244, 245, 282). Dolayısıyla işlenen eylemler yasanın aynı maddesini ihlal etmesine rağmen, aynı suçu oluşturmayabilmektedir. Bu bağlamda failin ilk önce mağdurun bilişimsistemini bozması (TCK m. 244/1), sonrasında ise bu bilişim sistemini kullanarak haksız yararelde etmesi halinde (TCK m.244/4) bu

26 Dülger, s.399.
27 Dülger, s.400.
28 Dülger, s.401.
29 Dülger, s.401.

eylemler aynı suç işleme kararı kapsamında gerçekleşseler dâhi, bunlar farklı suçlar oldukları, farklı hukuksal değerleri korudukları için zincirleme suç oluşmayacaktır. Aynı durum 244. maddenin 1. ve 2. fıkralarındaki suç tipleri arasındaki ilişki açısından da geçerlidir.[30]

f. Yaptırım, Soruşturma ve Kovuşturma

TCK'nın 244. maddesinin 1. ve 2. fıkralarında yer alan her iki suç için de yalnızca hürriyeti bağlayıcı ceza öngörülmüştür. Yasada bu suçların cezası olarak 1. fıkra açısından bir yıldan beş yıla kadar hapis cezası, 2. fıkra açısından ise altı aydan üç yıla kadar hapis cezası öngörülmüştür. Suçun düzenlendiği 244. maddenin 3. fıkrasında yer alan suçun nitelikli halinin gerçekleşmesi halinde ise faile verilecek olan ve alt ile üst sınırı yukarıda belirtilmiş olan cezalar yarı oranında artırılacaktır.

TCK'nın 244. maddesinin 4. fıkrasında yer alan bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunu işleyen failler için hem hürriyeti bağlayıcı ceza hem de Adlî para cezası öngörülmüştür. Yasada bu suçun cezası olarak iki yıldan altı yıla kadar hapis cezası ve beş bin güne kadar Adlî para cezası düzenlenmiştir. [31]

3.1.3. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçları (m.245)

"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) (Ek fıkra: 06/12/2006 - 5560 S.K.11.md) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır."

a. Korunan Hukuksal Değer

Banka veya kredi kartlarının kötüye kullanılması suçlarının aslında birçok suç tipinin "ratio legis"lerini taşıdığı maddenin gerekçesinde belirtilmiştir; buna göre "hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçları" ile korunmak istenilen hukuksal değerler TCK'nın 245. maddesinde düzenlenen inceleme konusu

30 Dülger, s.401.

31 Dülger, s.403.

suç tipleriyle korunmak istenen hukuksal değerleri oluşturmaktadır. Bunlardan hırsızlık ve dolandırıcılık suçları ile kişilerin malvarlığı, güveni kötüye kullanma suçu ile kişilerin birbirine karşı duyduğu kişisel güven, sahtecilik suçunda ise devlet tarafından fertlere yüklenilen hukuk alanında inandırıcılığı olan belgelere olan güven korunmak istenmektedir.[32]

b. Tipikliğin Maddî Unsurları

aa. Fail: Bu suçların faili herkes olabilir, yasada bu açıdan bir özellik gösterilmemiştir. Ancak özellikle sahte kredi veya banka kartı yapımında kullanılan araçların ve banka hesap bilgilerinin elde edilmesi ve kartlara uygulanması belli bir seviyede uzmanlık bilgisini gerektirmektedir. Ancak bu durum bu suçu işleyen ya da iştirak eden herkes için geçerli değildir. Uygulamada ortaya çıkan örneklerde de görüldüğü üzere bugün için bu suç tipi genellikle çete halinde işlenmektedir; çete üyelerinden de yalnızca birinin böyle bir uzmanlık bilgisine sahip olması eylemlerin gerçekleştirilmesi için yetmektedir.[33]

bb. Mağdur: Bu suçların mağdurunun belirlenmesi için öncelikle suç tipinde yer alan "kart sahibi" ve "kartın kendisine verilmesi gereken kişi" kavramlarının açıklanması gerekmektedir. 5237 sayılı TCK'nın yürürlüğe girmesinden sonra yürürlüğe giren "Banka Kartları ve Kredi Kartları Kanunu"nda (BKKKK), TCK'nın 245. maddesinde yer alan ifadelerden farklı olarak "kart hamili" ifadesi kullanılmıştır. BKKKK'da ise bu konu için "kartlı sistem kuruluşu", "kart çıkaran kuruluş" ve "kart hamili" ifadeleri kullanılmıştır. BKKKK'nın 3. maddesinde bu terimler tanımlanmıştır, buna göre "kartlı sistem kuruluşu": "Banka kartı veya kredi kartı sistemi kuran ve bu sisteme göre kart çıkarma veya üye iş yeri anlaşması yapma yetkisi veren kuruluşları", "kart çıkaran kuruluş": "Banka kartı veya kredi kartı düzenleme yetkisini haiz bankalar ile diğer kuruluşları", "kart hamili" ise: "Banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişiyi" ifade etmektedir.

BKKKK'da yer alan ifadelerden özellikle "kart hamili" karşısında TCK'da "kart sahibi" ifadesinin kullanılması aynı konuyu düzenleyen iki farklı yasa arasında çelişki oluşmasına yol açmıştır. Çünkü kart hamili kartın sahibi olmayıp yararlanıcısıdır. Banka ve kredi kartlarının gerçek sahibi banka veya kredi kuruluşlarıdır. Buna göre TCK'da yer alan kart sahibi ifadesi BKKKK'daki düzenleme dikkate alınarak kart hamili olarak anlaşılmalıdır. Benzer şekilde "kartın kendisine verilmesi gereken kişi" de kart hamili olan kişidir. Nitekim uygulamada bu ifadeler kartın hamili olarak algılanmaktadır. Ancak tipe uygunluğun sağlanması için maddede yapılacak bir düzenleme ile bu hususlar BKKKK ile uyumlu olacak şekilde değiştirilmeli ve kart hamili ifadesi yasa maddesine alınmalıdır.[34]

cc.Suçun Konusu: Suçun konusu banka kartı ve kredi kartlarıdır.[35]

dd. Eylemler:

aaa. Başkasına Ait Banka veya Kredi Kartıyla Hukuka Aykırı Yarar Sağlanması (245/1): Suçun gerçekleşmesi için öncelikle banka veya

32 Dülger, s.420.
33 Dülger, s.422.
34 Dülger, s.423.
35 Dülger, s.428.

kredikartının fail tarafından ele geçirilmesi veya elde bulundurulması gerekmektedir. Ancak tek başına bu hareketlerin yapılması suçun eylem unsurunun gerçekleşmesi için yeterli değildir. Bunun akabinde failin kartı kullanarak ya da kullandırtarak haksız bir yarar elde etmesi gerekir. Dolayısıyla suç tipi serbest hareketli ve birleşik şekilde düzenlenmiştir. Buna karşın ele geçirme, elde bulundurma, kullanma ve kullandırtma hareketlerinin nasıl yapılacağı konusunda bir sınırlandırma yapılmamıştır, önemli olan birleşik olarak gerçekleştirilen bu hareketlerin neticesinde haksız yararın elde edilmesidir. Dolayısıyla hareketler kendi içinde serbest şekilde düzenlenmiştir.[36]

bbb. Başkalarına Ait Banka Hesaplarıyla İlişkilendirilerek Sahte Banka veya Kredi Kartı Üretilmesi, Satılması, Devredilmesi, Satın Alınması veya Kabul Edilmesi: 245. maddenin 2. fıkrasında başkalarına ait banka veya kredi kartıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması devredilmesi, satın alınması veya kabul edilmesi hareketleri ayrı bir suç olarak düzenlenmiştir. Banka veya kredi kartlarının tamamen sahte olarak üretilmesi mümkün olduğu gibi, bu kartların gerçek olmasına rağmen üzerinde çeşitli işlemler yapılarak sahteleştirilmesi de mümkündür. Bu durum yasa koyucu tarafından iyi bir şekilde tespit edilerek suç tipine yansıtılmıştır.

Suç tipi seçimlik hareketli olarak düzenlenmiştir, bu hareketlerden her hangi birinin yapılması ya da bazı hareketlerinin birlikte yapılması halinde 245/2. maddenin ihlali söz konusu olacaktır. Örneğin, failin önce sahte kartı üretmesi ve sonrasında satması halinde tek bir suç oluşacaktır. Ancak üreten ve akabinde satan ile satın alan ayrı kişiler olduğunda bunların herbiri açısından ayrı ayrı 245/2. maddenin ihlali söz konusu olacak, bunlar arasında suça iştirak hâli söz konusu olmayacaktır.[37]

ccc. Sahte Oluşturulan veya Üzerinde Sahtecilik Yapılan Bir Banka veya Kredi Kartını Kullanmak Suretiyle Yarar Sağlanması: 245. maddenin 3. fıkrasında yer alan suç ile 2. fıkrada belirtilen sahte olarak üretilen ya da gerçek bir kart üzerindeki işlemlerle sahteleştirilen kartların kullanılması suretiyle haksız yarar sağlanması eylemleri cezalandırılmaktadır. Suç tipi serbest hareketli olarak düzenlenmiştir, sahte olduğunu bilerek banka veya kredi kartını kullanmak suretiyle haksız yarar sağlayan failin bu fıkra kapsamında cezalandırılabilmesi için ayrıca suça konu olan kartı sahte olarak üretmesi veya üzerinde sahtecilik yapması gerekmemektedir, bu tür kartlarla haksız yarar elde edilmesi suçun oluşması için yeterlidir.[38]

c. Tipikliğin Manevî Unsurları

245. maddenin 1., 2., ve 3. fıkralarında yer alan her suç tipi açısından suçun manevi unsurunu kast oluşturmaktadır. Suçta manevi unsur açısından bir başka unsur aranmamıştır.[39]

d. Hukuka Aykırılık Unsuru

Failin yarar sağladığı hareketleri bir rızaya dayanarak gerçekleştirdiği durumda suç oluşmayacaktır, çünkü yasada açık bir şekilde "kart sahibinin veya kartın

36 Dülger, s.432.
37 Dülger, s.442.
38 Dülger, s.452.
39 Dülger, s.457.

kendisine verilmesi gereken kişinin rızası olmaksızın" yarar sağlanması halinde failin cezalandırılacağı belirtilmiştir. Bu durumda kart sahibinin ve kartın kendisine verilmesi gereken kişinin rızası eylemi suç olmaktan çıkarmaktadır.[40]

e. Suçun Özel Görünüş Biçimleri

aa. Teşebbüs: 245. maddenin 1. ve 3. fıkralarında yer alan suç tiplerinde suçun tamamlanması için failin suç tanımında yer alan hareketleri yapmasının yanı sıra "haksız yarar elde etmek" şeklindeki neticeyi de gerçekleştirmesi gerekmektedir. Fail tarafından hareketlerin tamamlanması ancak neticenin gerçekleşmemesi hâlinde suç teşebbüs aşamasında kalmış olacaktır.[41]

245. maddenin 2. fıkrasında yer alan suç açısından ise, durum daha farklıdır. Bu suç açısından failin yaptığı hareketlerin sonucunda ayrıca bir neticenin gerçekleşmesi aranmamaktadır. Dolayısıyla failin suç tanımında yer alan hareketleri yapması ile suç gerçekleşmektedir. Buna göre failin yapmış olduğu hareketlerin parçalara bölünebilmesi halinde suç teşebbüs aşamasında kalmış olacaktır.

bb. İştirak: 245. maddenin 1., 2. ve 3. fıkralarında yer alan suçlara iştirak açısından bir özellik söz konusu olmayıp TCK'nın 37., 38., 39. ve 40. maddelerinde düzenlenen suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir; bu suçlar açısından iştirakin her hali mümkündür.[42]

f. Yaptırım, Soruşturma ve Kovuşturma

245. maddenin 1. fıkrasında tanımlanan "başkasına ait bankaveya kredi kartıyla hukuka aykırı yarar sağlama" suçunun gerçekleştirilmesi halinde faile üç yıldan altı yıla kadar hapis ve beş bin güne kadar Adlî para cezası verilmesi öngörülmüştür. Görüldüğü üzere aradaki "ve" bağlacı nedeniyle hapis ve Adlî para cezaları seçenek yaptırımlar olarak değil, ikisi birlikte uygulanmak üzere düzenlenmişlerdir.

Maddenin 2. fıkrasında yer alan "sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartıyla hukuka aykırı yarar sağlama" eyleminin gerçekleştirilmesi halinde ise faile dört yıldan yedi yıla kadar hapis cezası verilecektir. Yasa koyucu bu eylem açısından Adlî para cezası öngörmemiştir.[43]

"Bir şekilde elde etiği mağdura ait kredi kartı bilgilerini kullanarak cep telefonuna kontör yüklemek ve internet üzerinden alışveriş yapmak suretiyle haksız yarar sağlamak şeklinde gerçekleşen olayda.. eylemin TCK'nın 245/1. Maddesinde tanımlanan "banka ve kredi kartlarının kötüye kullanılması" suçunu oluşturacağı, mağdura ait kredi kartının sahtesi üretilerek kullanıldığına dair herhangi bir tespit ve delil de bulunmadığı gözetilmedeni suç vasfında yanılgı sonucu TCK'nın 243/3. Maddesinin uygulanması suretiyle yazılı şekilde fazla ceza tayini (bozulmasını gerektirmiştir). 11. CD., Kt. 4.6.2013, E. 2012/2220, K.2013/9277.

40 Dülger, s.458.
41 Dülger, s.460.
42 Dülger, s.464.
43 Dülger, s.511.

3.2. Bilişim Sisteminin Kullanılmasının Suçun Nitelikli Hâli Olarak Düzenlendiği Suçlar

3.2.1. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Hırsızlık Suçu (TCK m.142/2-e)

a. Korunan Hukuksal Değer

Bu suçla korunan değer kişilerin malvarlığı bir başka deyişle mülkiyet hakkıdır.[44]

b. Tipikliğin Maddî Unsurları

aa. Fail: Bu suçun faili herkes olabilir, fail açısından bir özellik aranmamıştır.[45]

bb. Mağdur: Bu suçun mağduru malvarlığında azalma olan, bilişim sistemi suretiyle veri şeklindeki parası transfer edilen kişilerdir. Ancak bu suç tipi açısından özellikle üzerinde durulması gereken konu, genellikle bankalarda yer alan hesaplar üzerinde bu suçlarınişlendiği de dikkate alınarak, bu suçların mağdurunun bankaların mı yoksa bankada hesabı bulunan kişiler mi olduğudur. Bu sorunun yanıtlanması için kişi ile banka arasındaki sözleşmenin niteliği incelenmelidir.[46]

cc.Suçların Konusu: Bu suçun konusunu "veri" oluşturmaktadır. Kişisel olsun olmasın bilişim sistemleri kullanılmak suretiyle hırsızlık eylemine hedef olan veriler bu suçun konusunu oluşturmaktadır. Buna göre sisteme bağlantısı olmayan bir veri bu suçun konusunu oluşturmayacaktır. O halde bilişim sisteminin kullanılmadığı, harici bir hard diskin içinde bulunan verinin ele geçirilmesi amacıyla bu hard diskin alınması halinde 244/2 maddesi, bundan bir haksız yarar elde edilmesi halinde ise 244/4 maddesi uygulanacaktır.

TCK'nın 142/2-e maddesinde "bilişim sistemlerinin kullanılması suretiyle hırsızlık"tan söz edilmektedir. Burada, bilişim sisteminin sağladığı benzersiz olanaklar nedeniyle, hırsızlık suçunun çok daha kolay işlenebilmesi olgusu gözetilmektedir. Düzenlemede esas olan, verinin çalınmasından önce, hırsızlık suçunda bilişim sisteminin kullanılmış olmasıdır. Diğer yandan, nasıl ki elektrik enerjisi nesnel bir yapıya sahip olmadığı halde hırsızlığa konu olabiliyorsa, "veri" için de benzer yaklaşım pekâlâ mümkündür. Kaldı ki "veri"nin de sonuçta ekonomik bir değeri vardır. Yaşamakta olduğumuz bilgi çağının bir gereği olarak yeni bir yaklaşımla veri, hırsızlık suçuna konu olabilecektir.[47]

dd. Eylemler: Hırsızlık suçunun oluşması için taşınır malın bulunduğu yerden alınması gerekir. Bir malın zilyedinin egemenlik alanından çıkarılıp failin egemenlik alına sokulmasıyla alma gerçekleşmiş olur. Burada üzerinde durulması gereken husus, failin suçun konusu olan mal üzerinde serbestçe tasarrufta bulunabilecek konuma ulaşmış olmasıdır. Böylelikle asıl zilyedin suçun konusu olan mal üzerinde tasarrufta bulunması olanaksız hale getirilmiş olmaktadır. Suçun bilişim sistemleri kullanılmak suretiyle gerçekleştirilen nitelikli halinde de suçun temel şeklinde olduğu gibi malın

44 Dülger, s.517.
45 Dülger, s.517.
46 Dülger, s.517.
47 Dülger, s.517.

(eşya, para vb.) zilyedinin hâkimiyet alanından çıkması gerekmektedir. Ancak bu durumda "alma" hareketi fiziksel olarak değil, bilişim sistemleri kullanılmak suretiyle ve sanal alanda söz konusu olmaktadır. Bu da uygulamada oldukça çok görülen bir maddedir.[48]

c. Tipikliğin Manevi Unsuru

Bu suç ancak kast ile işlenebilir, maddede açıkça belirtilmediği için taksirle işlenmesi mümkün değildir.[49]

d. Hukuka Aykırılık Unsuru: Bilişim yoluyla hırsızlığa maruz kalan mağdurun, parasının aktarıldığı sanığın ya da üçüncü bir kişinin banka hesabından aynı şekilde para çalması hâlinde, haklı savunma halinin varlığından söz etmek, bu kurumun içeriğiyle ve yasada düzenlenme amacıyla bağdaşmaz. Dolayısıyla bu durumda haklı savunmadan söz edilemez. İkinci eylemin kendisi de nitelikli hırsızlık suçunu oluşturacaktır.[50]

e. Suçun Özel Görünüş Biçimleri

aa. Teşebbüs: Bu suç parçalara bölünebildiğinden teşebbüs aşamasında kalması mümkündür. Çünkü suçun tamamlanması için malın alınması ya da very halindeki paranın transfer edilmesi yetmeyip failin egemenlik alanına girmesi de gerekmektedir. Bu ise belli bir zaman gerektirdiğinden, bu zaman esnasında hareketin yarıda kalması halinde suç teşebbüs aşamasında kalmış olacaktır. Ancak hemen belirtelim ki, suçun bilişim sistemleri suretiyle işlenmesi hâlinde veri şeklindeki paranın transferi ile failin hâkimiyet alanına girmesi arasında saniyelerle ölçülebilecek bir zaman dilimi olacağından suçun teşebbüs aşamasında kalmasına sıklıkla rastlanmamaktadır.[51]

bb. İştirak: Hırsızlık suçu iştirak bakımından bir özellik göstermemektedir, dolayısıyla bu suça iştirakin her türlüsü mümkündür.[52]

cc. İçtima: İnternetüzerinden yetkisiz erişimle bankanın online sistemine girilerek müşterilerin mevduat ya da kredi hesaplarından para transferi yapılması yukarıda da belirttiğimiz üzere YCGK'nın kararından sonra yerinde olarak 142/2-e maddesi içinde değerlendirilmektedir. Bu durumda failin parayı temsil eden veri hırsızlığını yapmadan önce bankanın bilişim sistemine girmesi ve sistemde kalması gerekmektedir. Dolayısıyla fail 142/2-e maddesindeki suçu işlemeden önce 243. maddede tanımlanan eylemi de gerçekleştirmektedir. Dolayısıyla bu iki madde arasındaki ilişkinin ortaya konulması gerekir.Burada ilk akla gelen bu suçlar açısından geçit suçunun söz konusu olup olmadığıdır. Geçit suçu, bir suçun işlenmesi için öncelikle cezası daha hafif olan bir suçun işlenmesinin, bu suçtan geçilmesinin gerekmesidir. Ancak geçit suçunun söz konusu olabilmesi için işlenen ilk suçun ve sonraki daha ağır suçun aynı hukuksal değeri koruması gerekir. Oysa 243. maddede bilişim sisteminin güvenliği korunmakta iken 244/2-e'de mağdurun malvarlığı korunmaktadır. Dolayısıyla bu iki suç arasında korunan hukuksal değerlerin farklı

48 Dülger, s.540.
49 Dülger, s.551.
50 Dülger, s.541.
51 Dülger, s.542.
52 Dülger, s.542.

olması nedeniyle geçit suçunun gerçekleşmesi mümkün değildir. Diğer yandan geçit suçunun söz konusu olabilmesi için ilk suçtan geçilmeksizin ikinci suçun işlenememesi gerekir (örneğin kasten yaralama suçu işlenmeden kasten öldürme suçunun işlenmesi mümkün değildir). Her iki suç bu açısından incelendiğinde bilişim sistemi aracılığıyla hırsızlık suçunun işlenmesi için, mutlaka sisteme girme ve orada kalmaya devam etme suçunun işlenmesi gerekmemektedir. Zîra 243. maddedeki eylemin suç oluşturması için bunun hukuka aykırı olarak gerçekleştirilmesi gerekir, bu eylemlerin mağdurunun rızasıyla işlenmesi halinde ise hukuka aykırılık unsuru ortadan kalkacağı için suç da gerçekleşmeyecektir. Örneğin bankanın bilişim sisteminin test edilmesi ya da bakım yapılması için bilişim güvenliği uzmanlarına yetki verilmesi halinde sisteme giriş ve sistemde kalma hukuka uygun olmakta ve suç oluşmamaktadır. İşte bu kişilerin sistem içindeki verilerin transferi yoluyla hırsızlık yapmaları hâlinde (bu kişilerin banka çalışanı olmağı da dikkate alındığında) 142/2-e'de tanımlanan suç gerçekleşmiş olacak ancak 243. maddedeki suç işlenmemiş olacaktır. Dolayısıyla bilişim sistemleri aracılığıyla hırsızlık suçunun işlenmesi için mutlak surette bilişim sistemine girme ve sistemde kalmaya devam etme suçunun işlenmesine gerek bulunmamaktadır. Sonuç olarak bu açıdan da her iki suç arasında geçit suçu ilişkisinin bulunmadığı görülmektedir. Bu eylemlerin birlikte gerçekleştirilmesi hâlinde faile her iki suçun da cezası verilmelidir.[53]

dd. Yaptırım, Soruşturma ve Kovuşturma: Hırsızlık suçunun temel hali için bir yıldan üç yıla kadar hapis cezası öngörülmüşken, 142/2-e'deki suçun nitelikli hali için üç yıldan yedi yıla kadar hapis cezası öngörülmüştür. Bu suçun temel hali açısından da nitelikli hali açısından da aslîye ceza mahkemeleri yargılama yapmakla görevlidir.[54]

"Sanıkların, hakkındaki dosya tefrik edilen S.D. isimli sanıkla internet yoluyla yakınana ait hesaba girip, 2.07,99 TL parayı sanık C.Ş.'in hesabına transfer etmeleri şeklinde gerçekleşen olayda; eylemin TCK'nın 142/2-e maddesinde düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden, suçun vasıflandırılmasında yanılgıya düşülerek yazılı şekilde karar verilmesi (Bozmayı gerektirmiştir.)" 6. CD., Kt. 20.6.2013, E. 2013/10638, K. 2013/14137.

3.2.2. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Dolandırıcılık Suçu (m.158/1-f)

TCK'nın malvarlığına karşı suçlar başlıklı onuncu bölümünün 157. maddesinde dolandırıcılık suçu, 158. maddesinde ise dolandırıcılık suçunun nitelikli halleri düzenlenmektedir. Bu maddenin 1. fıkrasının (f) bendinde "bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık suçu" yer almaktadır. Buna göre: "(1) Dolandırıcılıksuçunun; ... f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle, ... işlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar Adlî para cezasına hükmolunur..."

Bu suçla hem bireylerin malvarlıkları, hem irade özgürlükleri, hem de toplumsal yaşam içinde diğer insanlara duydukları güven korunmaktadır.

Dolandırıcılık suçu fail ve mağdur açısından bir özellik göstermemektedir, herkes bu suçun faili ve mağduru olabilir.

53 Dülger, s.542.

54 Dülger, s.544.

Yargıtay kararlarına göre bilişim suretiyle dolandırıcılık suçunun gerçekleşebilmesi için suçun eylem unsuru olan hilenin gerçek kişiye yönelmesi, mağdurun hataya düşürülerek kendi veya bir başkasının malvarlığı aleyhine, sanık veya bir başkasının lehine bir işlemde bulunmaya yöneltilmesi ve bu işlem sonucunda sanığın kendine veya başkalarının yararına haksız bir yarar sağlaması gerekmektedir. Nitekim Yargıtay istikrarlı bir şekilde bu durumlarda dolandırıcılık suçunun oluşmadığını belirtmekte ve eylemleri diğer suçlar açısından incelemektedir. Örneğin mail-order yöntemi kullanılarak kredi kartlarıyla haksız yarar elde edilmesinde gerçek kişiye yönelik bir hilenin söz konusu olmasının gerektiğini belirterek bu durumda bilişim sistemleri suretiyle dolandırıcılık suçunun değil başkasının banka veya kredi kartıyla haksız yarar elde edilmesi suçunun oluştuğu yönünde karar vermiştir.[55] Bu görüş öğreti tarafından da paylaşılmaktadır.

Uygulamada en sık karşılaşılan bilişim sistemleri aracılığıyla dolandırıcılık eylemleri, failin bir kişiye ait sosyal medya (MSN massenger, facebook vd.) ya da elektronik posta giriş şifrelerini ele geçirerek şifresini ele geçirdiği kişilerin arkadaşlarına kendisini profil sahibi gibi tanıtıp para istemesi ya da belli bir telefona kontör yüklenmesini talep etmesi ve istemlerinin kabul edilmesi suretiyle gerçekleştirilmektedir. Fail burada, profilin arkadaşları ya da yakınları olan mağdurların iyi niyetinden, güveninden ya da bazen saflığından faydalanarak haksız yaara elde etmektedir. Bilişim suçları dünyasında bu yönteme "phishing" denilmektedir ve ülkemizde de yabancı ülkelerde de en sık görülen dolandırıcılık yöntemlerinden biridir.[56] En kısa tanımı ile phishing şifre avcılığıdır; spam göndericileri tarafından uygulanan bu yöntemde kullanıcıya gönderilen elektronik posta ile bilgilerini güncellemesi istenmekte ve posta içinde hazırlanmış kutulara ya da tıklanınca açılan gerçek görünümlü sahte sitedeki kutulara kullanıcı adı ve şifre gibi bilgilerin girilmesi sağlanmaktadır.

Dolandırıcılık suçunun oluşması için haksız yarar sağlanması, suçun teşebbüs aşamasında kaldığının kabul edilebilmesi için hazırlık hareketlerinin sona erip haksız yararın elde edilmesine yönelik icra hareketlerine başlanması gerekmektedir.

Bilişim sistemleri kullanılmak suretiyle işlenen dolandırıcılık suçunun cezası üç yıldan yedi yıla kadar hapistir. Ayrıca bu suçun cezası olarak hapis cezasının yanında adlî para cezasına hükmedilmesi gerekmektedir. Nitelikli dolandırıcılığın bu türü için beş bin güne kadar Adlî para cezası öngörülmekle birlikte adlî para cezasının miktarının suçtan elde edilen yararın iki katından az olamayacağı belirtilmiştir.[57]

"Katılana ait olan Ziraat Bankası S... şubesi nezdindeki internet şubesi hesabına sanığın, haksız yere elde ettiği katılana ait şifre ile girerek, 2.080 TL parayı yeğeni olan tanık S.M.'a yatırdığı, 24.4.2006 günü ise 6.577 TL parayı kendi hesabına aktardığının anlaşılması karşısında, sanığın eylemi 5237 sayılı TCK'nın 142/2-e maddesindeki suçu oluşturduğu halde aynı Kanunun 158/1-f maddesiyle uygulama yapılması.. BOZMAYI gerektirmiştir." 13. C.D., Kt. 11.6.2013, E. 2013/3821, K. 2013/17985. Kazancı İçtihat Bilgi Bankası.

55

56

57 Dülger, s.544.

3.3. Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Suçlar

3.3.1. Ödeme Sistemleri BKK 23, 39, Banka Kartları Ve Kredi Kartları Kanununda Düzenlenen Suçlar

a. Genel Olarak

Banka ve kredi kartları sisteminin etkin bir şekilde çalışmasını sağlamak amacıyla, 1 Mart 2006 Tarihli Resmî Gazete'de yayımlanmak suretiyle, 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu yürürlüğe girmiştir. Kanun öncesi mevzuatımızda özel bir düzenleme bulunmaması nedeniyle banka ve kredi kartlarıyla ödeme sisteminde ve sistemin tarafları arasında çeşitli hukukî ihtilaflara neden olmaktaydı. Ortaya çıkan hukukî ihtilafların yanında, banka veya kredi kartlarının suça konu olması ceza kanunlarındaki düzenlemelerin ortaya çıkan ihlalleri tanımlamaması nedeniyle Ceza Hukuku'nun temel prensiplerinden olan kanunilik ilkesi ve kıyas yasağı nedeniyle çoğu eylemin yaptırımsız kalmasına neden olmaktaydı.

5237 sayılı TCK'nın 245. maddesinde banka ve kredi kartlarının kötüye kullanılmasını engellemeye yönelik düzenlemeye paralel hükümleri de beraberinde getiren, özel bir düzenleme mevzuatımıza girmiştir.

b. Kanunda Düzenlenen Suçlar

Banka Kartları ve Kredi Kartları Kanunu genel olarak, kartlı ödeme sistemlerinde ortaya çıkan hukukî sorunlara çözüm bulmak, sistemin tarafları olan kişi ve kurumların hak ve sorumluluklarını tespit etmek ve bu şekilde sistemin güvenilir ve etkin bir şekilde çalışmasını sağlamak amacıyla hayata geçirilmiştir. Ancak bunun yanında, 5237 Sayılı TCK'nın 245. maddesinde düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun tamamlayıcısı şeklinde düzenlenen suçlarla ilgili düzenlemelere de kanunda yer verilmiştir.

aa. Sahte Belge Düzenlenmesi:

5464 sayılı Kanun

Madde 36 - *Gerçeğe aykırı olarak harcama belgesi, nakit ödeme belgesi ya da alacak belgesi düzenlemek veya bu belgelerde ne surette olursa olsun tahrifat yapmak suretiyle kendisine veya başkasına yarar sağlayanlar, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılırlar.*

Kanun maddesinde bahsi geçen harcama belgesi, nakit ödeme belgesi ve alacak belgesi ile ilgili tanımlamaları yapmak gerekirse;

Harcama Belgesi (Satış Belgesi, Slip): Banka kartı veya kredi kartı ile yapılan işlemler ile ilgili olarak üye iş yeri tarafından düzenlenen, kart hamilinin işlemden doğan borcu ile diğer bilgileri gösteren ve kart hamilinin kimliğinin bir kod numarası, şifre veya kimliği belirleyici başka bir yöntemle belirlendiği haller dışında kart hamili tarafından imzalanan belgedir.

Nakit Ödeme Belgesi: Bankalarca veya yetkili üye işyerlerince banka kartı veya kredi kartı hamiline yapılan nakit ödemelerde düzenlenerek, kart hamilinin

kimliğinin bir kod numarası, şifre veya kimliği belirleyici başka bir yöntemle belirlendiği haller dışında kart hamili tarafından imzalanan belgedir.

Alacak Belgesi: Banka kartı veya kredi kartı kullanılarak alınmış olan malın iadesi veya hizmetin alımından vazgeçilmesi veya yapılan işlemin iptali halinde kart hamilinin hesabına alacak kaydedilmek üzere üye iş yeri tarafından düzenlenen belgedir, şeklinde tanımlanabilir.

Esas itibariyle bahse konu suçun, özel belgede sahtecilik ve dolandırıcılık suçunun unsurlarını içinde bulunduran, başka bir deyişle sahtecilik ve dolandırıcılık suçlarından oluşan bileşik bir suç olarak değerlendirilebilmesi mümkündür.

Suç, gerçeğe aykırı olarak harcama belgesi, nakit ödeme belgesi ya da alacak belgesi düzenleyerek veya bu belgelerde ne surette olursa olsun tahrifat yapmak suretiyle kendisine veya başkasına yarar sağlamak şeklinde gerçekleşmektedir.

Banka Kartları ve Kredi Kartları Kanunu'nun 36. maddesinde düzenlenen bu suç, seçimlik hareketli bir suç olarak düzenlenmiştir. Gerçekte satış, nakit ödeme ve mal iadesi veya hizmet alımından vazgeçilmesi söz konusu olmadığı halde yapılmış gibi harcama belgesi, nakit ödeme belgesi ve alacak belgesi düzenlemek veya bahse konu bu belgelerde her ne surette olursa olsun tahrifat yapmak suretiyle, kendisine veya başkasına yarar sağlanması durumunda bu suç işlenmiş sayılacaktır.

Suçla korunan hukukî değer açısından belgede sahtecilik suçlarında olduğu gibi kamu güveninin yanında genel olarak malvarlığı hakkı ve suçun düzenlenmiş olduğu kanunun genel amacı kapsamında kartlı ödeme sisteminin korunduğunu söylemek mümkündür.

Suçun faili ise kural olarak herkes olabilmektedir. Bu suçun mağduru ise, kural olarakkartlı sistem kuruluşları, kart çıkaran kuruluşlar bankalar veya kart hamilleri olabilir.

Kasten islenebilen bu suçun gerçekleşmesi için, failin, gerçeğe aykırı olduğunu bildiği harcama belgesi, nakit ödeme belgesi veya alacak belgesini bilerek ve isteyerek düzenlemenin yanında, bu gerçeğe aykırı belgeyi kullanma neticesinde kendisine veya başkasına yarar sağlama kastıyla hareket etmesi yeterli olmaktadır. Bununla beraber, gerçeğe aykırı belgeyi oluşturmuş fakat kullanma neticesi bir şekilde yarar sağlayamamış fail açısından teşebbüs hükümlerinin uygulanabileceği açıktır. Bu suç teşebbüse elverişli bir suçtur.

İştirak açısından suçun herhangi bir özelliği bulunmamaktadır. Yani bu suça iştirakin her türlüsü mümkün olmaktadır. Bununla beraber, uygulamada çoğunlukla üye iş yeri çalışanları bu suçu birlikte isledikleri gibi, daha önce de belirtildiği üzere, kart hamilleri veya üçüncü kişilerce anlaşarak da işleyebilmekte, başka bir deyişle suçun iştirak hâlinde işlendiğini pek çok şekilde görmek mümkün olmaktadır. İçtima hükümleri açısından da suçla ilgili özel bir düzenleme mevcut değildir. Suçun değişik zamanlarda aynı suç isleme kastıyla bir kişinin veya kuruluşun zararına birden fazla işlenmesi durumunda zincirleme suçtan söz edilebilirken, birden çok kişinin veya kuruluşun zararına işlenmişse, gerçek içtima hükümleri çerçevesinde kişi ya da kuruluş adedince suçun gerçekleştiği kabul edilecektir. Son olarak, fikri içtima hükümleri esas alınarak aynı eylemle başka bir suçun da işlenmesi durumunda fail hakkında daha ağır

cezayı gerektiren suçtan hüküm kurulabileceğini de belirtmek gerekir.

bb. Gerçeğe Aykırı Beyan, Sözleşme ve Eki Belgelerde Sahtecilik:

5464 Sayılı Kanun

Madde 37 - *Banka kartı veya kredi kartını kaybettiği ya da çaldırdığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile bunları bilerek kullananlar bir yıldan üç yıla kadar hapis ve ikibin güne kadar adlî para cezası ile cezalandırılırlar.*

Kredi kartı veya üye iş yeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler.

Banka Kartları ve Kredi Kartları Kanunu'nun 37. maddesinde iki fıkra hâlinde iki suç düzenlenmektedir. Bunlardan birincisi banka veya kredi kartını kaybettiği ya da çaldırdığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile kart hakkındaki gerçek olmayan beyandan haberdar olan üçüncü kişilerin cezalandırılacağına ilişkindir.

İkincisi ise, kredi kartı veya üye iş yerisözleşmesinde veya eki belgelerde sahtecilik yapanların veya sözleşme imzalamak maksadıyla sahte belge ibraz edenlerin cezalandırılacağına ilişkindir.

Birinci fıkrada düzenlenen suçla ilgili madde gerekçesinde kart hamilleri tarafından kartların kullanımının suistimal edilmesini engelleme amacından bahsedilmiştir.

Ülkemiz uygulamasında, kart hamilinin sorumluluğu 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu (md. 12) ile sınırlandırılmıştır. Ancak, bazı kurumlar tarafından çıkarılan kredi kartlarında yitik ya da çalınma gibi istek dışında elden çıkma durumları için kart hamili yararına üçüncü kişilerce yapılacak harcamaların sigorta kapsamına alındığı görülmektedir.Bugüne kadar, bu tür eylemlerde kredi kartı, kartın gerçek dışı kayıp bildiriminden sonra kullanılması nedeniyle eylemden bankanın zarar gördüğü ve eylemin bankaya karşı dolandırıcılık suçunu oluşturduğu kabul edilmekteydi. Mağdur banka kamu bankası ise, 765 sayılı TCK md. 504/7, özel banka ise 765 sayılı TCK md. 503/1 uygulanmaktaydı. Gerçekten dikkat edildiği takdirde kart hamilinin kart çıkaran kuruma karşı yalan beyanda bulunmak suretiyle hile yaptığı açıktır. Ancak burada dikkat edilmesi gereken ilk husus, kanun koyucunun, sadece bahse konu kartı kullanmak veya kullandırmak seklinde suçun oluşacağı ve bunun dışında dolandırıcılık suçunda olduğu gibi bir yararın elde edilmesini aranmadığı hususudur.

Kartın kullanılması neticesinde muhakkak bir yarar elde etme hedefi vardır fakat yarar elde edilmesi halinde fail ya da failler hakkında dolandırıcılık suçundan da hüküm kurulması gerektiğini söylemek gerekir. Zîra bu suçta sadece kartın kullanılması suçun oluşması açısından yeterli bulunmuştur.

Bu suçun faili kural olarak kart hamili olan herkes olabilir. Bunun yanında açıkça yer verilen"kullandırtma" kavramından hareketle kart hamili olmayan üçüncü şahısların da fail olabileceğini söylemek gerekir. Mağduru ise kart çıkaran kuruluşlar

veya bankalardır. Suçun konusu ise, banka veya kredi kartıdır. Kasten işlenebilen bu suçun üçüncü bir kişi tarafından islenebilmesi için, bu kişinin kartla ilgili bildirimi daha doğrusu kartın durumunu biliyor olması gerekir. Bu özelliğini bilmeden kartı kullanan kişi için bu suçun oluşması mümkün değildir.

Birinci fıkrada düzenlenen suça teşebbüs mümkündür. Fail gerçek dışı beyandan sonra kartın kullanımı esnasında yakalandığı takdirde teşebbüsten söz edilecektir. İştirakle ilgili olarak iştirakin her türlüsü mümkündür. Zaten kartın başkasına kullandırılması durumunda kart hamiliyle birlikte kartı kullanan da doğrudan bu suçun faili olmaktadır.İçtima hükümleri açısından ise, kart hamili birden fazla kartı birden fazla kart çıkaran kurum ya da bankanın zararına kullanmışsa, suçtan zarar gören adedince başka bir ifadeyle kullanım adedince suçun gerçekleştiği kabul edilerek, gerçek içtima kuralları çerçevesinde hüküm kurulacakken, aynı kartla farklı zamanlarda kullanım halinde zincirleme suçun varlığı kabul edilecektir. Son olarak; aynı eylem kanunda tanımlanan başka bir suçu da oluşturuyorsa burada fikrî içtima kuralları doğrultusunda fail ya da failler hakkında, işlemiş oldukları suçtan hangisi daha ağır ceza öngörüyorsa ondan hüküm tesis edilebilecektir.

Maddenin ikinci fıkrasında ise, 5237 sayılı TCK' da düzenlenen sahtecilik suçunun özel bir düzenlemesi yer almaktadır. Burada, tüm belgelerde değil fakat kredi kartı sözleşmesi, üye iş yeri sözleşmesi ve bunların ek belgelerinde sahtecilik yapılmasının yanında bahse konu sözleşmeleri düzenlemek amacıyla sahte belge ibraz edilmesi söz konusu olmaktadır. Burada sözü edilen sahtecilik sözleşmelerin yapılmasına ilişkin olup başka amaçla yapılan sahtecilik eylemleri bu fıkra kapsamında değerlendirilemeyecektir. Uygulamada kredi kartı kuruluşlarına veya genellikle bankalara, sahte ad ve belgeler sunmak suretiyle kart başvuruları yapıldığı sıklıkla karşılaşılan bir durumdur. Başvuru sahibi, kendi kimliğini gizleyerek, hayali ya da başka bir ad adına kredi kartı edinebilmektedir. Bazı durumlarda, kredi kartı başvurusu yapan kişi, gerçek kimlik bilgisini vermesine karşın, yüksek limitli kart alabilmek için ekonomik durumuna ilişkin gerçek dışı bilgi verebilir. Bu nedenle doğabilecek zararlardan kurtulabilmek için kart çıkaran kuruluşların basiretli bir tacir gibi davranarak işlemlerde gerekli özeni göstermesi yeterli olmamaktadır. Başvuran kişi hakkında olumlu istihbaratı bulunan banka, bir müddet sonra kredi kartını, faillerin bu iş için geçici olarak temin ettikleri bir adrese göndermektedir. Bu adreslere gönderilen kredi kartları ise hem nakit çekiminde, hem de alışverişte rahatlıkla şüphe çekmeden kullanılabilmektedir.

İkinci fıkrada düzenlenen suçla ilgili Yargıtay uygulamalarında sahte belgeler ibraz edilerek kart sözleşmesi tanzim edildikten sonra kartın basımı ile TCK'nun 245/2 maddesindeki suçun oluşacağı, kart basımının, talebin reddedilmesi nedeniyle gerçekleşmemesi durumunda ancak 5464 sayılı kanunun 37/2. maddesinin uygulama imkânı bulunduğu kabul edilmektedir.

cc. İzinsiz Kart Çıkarmak:

5464 Sayılı Kanun

Madde 38 - *Bu Kanunun 4'üncü maddesinde belirtilen izinleri almaksızın kartlı sistem kuran, kredi kartı çıkaran veya üye iş yeri anlaşması yapan veya ticaret unvanları, her türlü belgeleri, ilân ve reklamları veya kamuoyuna yaptıkları açıklamalarda bu işlerle uğraştıkları izlenimini yaratacak söz ve deyimleri kullanan*

gerçek kişiler ile tüzel kişilerin görevlileri bir yıldan üç yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılırlar.

Birinci fıkraya aykırılık halinde Kurumun, ilgili Cumhuriyet Başsavcılığını muhatap talebi üzerine sulh ceza hâkimince, dava açılması hâlinde davaya bakan mahkemece işyerlerinin faaliyetleri ve reklamları geçici olarak durdurulur, ilânları toplatılır. Bu tedbirler, hâkim kararı ile kaldırılıncaya kadar devam eder. Bu kararlara karşı itiraz yolu açıktır.

Banka Kartları ve Kredi Kartları Kanunu'nun 38. maddesiyle, gerekli izinleri almaksızın kartlı sistem kurulması, kredi kartı çıkarılması veya üye iş yeri anlaşması yapılması veya ticaret unvanları, her türlü belgeleri, ilan ve reklamları veya kamuoyuna yaptıkları açıklamalarla bu işlerle uğraştıkları izlenimini verecek söz ve deyimleri kullanmak şeklindeki eylemler yaptırım altına alınmıştır. Gerekli izinler ise aynı kanunun 4. maddesinde belirtilmiştir. İzinin alınacağı kurul ise aynı kanunun 3. maddesiyle Bankacılık Düzenleme ve Denetleme Kurulu olarak belirtilmiştir.

Sistemin güvenliği için, izin almaksızın kart çıkarılması veya benzeri faaliyetler yapılması ciddi bir tehdit unsuru oluşturabileceğinden, kanun koyucu isabetli olarak, bu tür faaliyetleri yaptırım altına almıştır. Bu suçu isleyenler için öngörülen hapis ve adlî para cezasının yanında, kuruluşlar için faaliyet ve reklamlarının geçici olarak durdurulması, ilanlarının toplatılması gibi tedbirlerde öngörülmüştür. Bu suç 5411 Sayılı Bankacılık Kanunu'nun 150. maddesinde düzenlenen 'izinsiz faaliyette bulunmak' suçuna paralel bir düzenleme olarak düzenlenmiştir.

Kartlı sistem kurma, kart çıkarma veya üye iş yeri anlaşması yapma şeklinde gerçekleşen eylemlerin suç olarak tanımlanabilmesi için, öncelikle izin alınmamış olması gerekir. Eğer kuruldan izin alınmışsa, bu suçun oluşmayacağı tartışmasızdır. Seçimlik hareketli olarak düzenlenen bu suç için, fail ya da faillerin, maddede yasaklanan eylemlerden birini yapması suçun oluşması için yeterli olacaktır. Ayrıca suçun oluşması için bir zarar unsuru aranmamıştır. Yani bu tip faaliyetlerden ötürü illa bir kişi veya bir kuruluşun zarar görmesi aranmamaktadır.

Suçun faili, gerçek kişiler ve tüzel kişilerin görevlileri başka bir deyişle herkes olabilir. Yani bu suç da aynı izinsiz faaliyette bulunmak suçu gibi, özgü bir suç değildir. Suçun mağduru ise, genel olarak tüm toplumdur Yine kasten işlenebilen bu suçun failinin, izinsiz olarak hareket ettiğini bilmesi suçun oluşması için yeterlidir. Taksirle işlenebilmesi ise, mümkün değildir.

İnceleme konumuz olan maddenin ikinci fıkrasında ise, "Birinci fıkraya aykırılık hâlinde kurumun, ilgili Cumhuriyet Başsavcılığını muhatap talebi üzerine sulh ceza hâkimince, dava açılması halinde davaya bakan mahkemece işyerlerinin faaliyetleri ve reklamları geçici olarak durdurulur, ilanları toplatılır. Bu tedbirler, hâkim kararı ile kaldırılıncaya kadar devam eder. Bu kararlara karşı itiraz yolu açıktır." ifadesiyle birinci fıkrada yasaklanan eylemlerle ilgili olan tüzel kişiler hakkında tedbirler belirtilmiştir.

dd. Bilgi Güvenliği Yükümlülüğüne Aykırı Davranılması:

5464 Sayılı Kanun

Madde 39 - *Bu Kanunun 8 inci maddesinin beşinci fıkrası ve 23 üncü*

maddesi hükümlerine kasten aykırı hareket eden kuruluşlar, üye işyerleri ve üye iş yeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevlileri ve işlemi yapan kişiler, bir yıldan üç yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılırlar.

Kartların kullanılması için zorunlu olup gizli kalması gereken kod numarası, kart numarası, şifre ya da kimliği belirleyici başka bir yöntemin dikkatsizlik veya tedbirsizlik veya meslekte yetersizlik veya emir ve kurallara aykırılık nedeniyle açığa çıkmasına neden olan kart çıkaran kuruluşlar, üye işyerleri ve üye iş yeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevli ve ilgili mensupları bin güne kadar adlî para cezası ile cezalandırılırlar.

Bu Kanunun 31 inci maddesine aykırı davrananlar hakkında bir yıldan üç yıla kadar hapis ve bin güne kadar adlî para cezası uygulanır.

Kartlı ödeme sistemin güvenli bir şekilde işlemesi için, kart hamillerine ait bilgilerin sadece kart hamili veya kart çıkaran kuruluşça bilinip, başkaları tarafından bilinmemesi gereklidir. Bu nedenle kanun koyucu tarafından, Banka Kartları ve Kredi Kartları Kanunu'nun 39. maddesi ile BDDK personelince, kart çıkaran kuruluş/bankalarca ve üye iş yerlerince bilinen ancak gizli kalması gereken bilgilerin açıklanması suç olarak düzenlenmiştir. Madde üç fıkradan oluşmaktadır.

İlk fıkrada; aynı kanunun 8/5. maddesine ve 23. maddesine kasten aykırı davranılması hâlinde, kasten aykırı hareket eden kuruluşlar, üye iş yerleri ve üye iş yeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevlileri ve işlemi yapan kişilerin bu eylemleri yaptırım altına alınmaktadır.

İkinci fıkrasında ise, yine 8/5 ve 23. maddelerine taksirle aykırı hareket eden kuruluşlar, üye işyerleri ve üye iş yeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevlileri ve işlemi yapan kişilerin eylemleri yaptırım altına alınmıştır. Son fıkrada ise, Kanunun 31. maddesine aykırı hareket eden kurul üyeleri ile kurum personeli ile kart çıkaran kuruluş ve üye iş yerlerinin bu eylemleri yaptırım altına alınmıştır.

Kanunun 8/5. maddesine göre, *"Kart çıkaran kuruluşlar, kartların kullanılması bir kod numarası, şifre ya da kimliği belirleyici başka bir yöntemin kullanılmasını gerektiriyorsa, bu tür bilgilerin gizli kalması amacıyla gerekli önlemleri almak ve harcama ve alacak belgesinin müşteri nüshası üzerinde ve yazışmalarda kart numarasının açıkça yer almasını engellemekle yükümlüdür." 23. maddesine göre ise; "Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye iş yeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye iş yeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle yükümlüdür. Kart çıkaran kuruluşlar, edindikleri kişisel ilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlüdür."* Bu sayılan yükümlülüklere kasten aykırı hareket edenler maddenin birinci, taksirlerle aykırı hareket edenler ise ikinci fıkrasına göre cezalandırılmaktadır.

Kanunun 8/5. maddesinde yaptırım altına alınan eylemler kart çıkaran

kuruluş ya da bankaların yöneticileri ve çalışanları tarafından, 23.maddesindeki eylemler ise üye iş yeri yöneticileri veya çalışanları tarafından islenebilmektedir. Üye iş yeri yöneticisi veya çalışanları edindikleri bilgileri kart hamilinin rızasıyla (ki bu yazılı izinle mümkündür) açıklar, saklar veya kopyalarsa bu suç oluşmaz. Maddenin ikinci fıkrasında ise '..dikkatsizlik veya tedbirsizlik veya meslekte yetersizlik veya emir veya kurallara aykırılık nedeniyle açığa çıkmasına neden olan' ifadesiyle, bahse konu yükümlülüklerin taksirle yerine getirilememesi de yaptırım altına alınmıştır.

Maddenin son fıkrasında ise Kanun'un 31. maddesinde iki fıkra halinde düzenlenmiş olan yükümlülüklere aykırı hareket edenlerin bu eylemleri yaptırım altına alınmıştır. 31. maddeye göre ise; *"Kurul üyeleri ile kurum personeli, görevleri sırasında öğrendikleri bu kanun kapsamındaki kuruluşlara, kart hamillerine ve kefillere ait sırları kanunen açıkça yetkili olanlardan başkasına açıklayamaz ve kendi yararlarına kullanamazlar." Ayrıca "kartlı sistem kuran, kart çıkaran, üye iş yeri anlaması yapan kuruluşlar, 29. maddede yer alan kuruluşlar ile üye işyerleri, bunların ortakları, yönetim kurulu üyeleri, mensupları, bunlar adına hareket eden kişiler ile görevlileri, sıfat ve görevleri dolayısıyla öğrendikleri sırları kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Kart çıkaran kuruluşların destek hizmeti aldığı kuruluş ve çalışanları hakkında da bu hüküm uygulanır."* Birinci fıkrada düzenlenen eylemler açısından kart hamili ve kefillere ait sırların açıklanması ve bunlardan yararlanılması, ikinci fıkrada düzenlenen eylemler açısından ise görev nedeniyle öğrenilen sırların açıklanması suç olarak düzenlenmiştir. İnceleme konumuz olan suçun failleri açısından konuyu değerlendirdiğimiz takdirde, maddede esas itibariyle birbirlerinden ayrı düzenlenmiş olan özgü suçlar düzenlendiğini görmek mümkündür. Bu suçun mağduru ise, sırrı veya bilgisi açıklanan, ifşa edilen ve menfaati ihlal edilen gerçek veya tüzel kişiler olmaktadır. Birinci ve üçüncü fıkrada düzenlenmiş suçlar kasten islenebilirken, ikinci fıkrada düzenlenen suç daha önce de ifade edildiği üzere taksirle islenmektedir. Birinci ve üçüncü fıkrada düzenlenmiş suçlara teşebbüs etmek mümkünken, taksirle islenme halini düzenleyen ikinci fıkradaki suça teşebbüs mümkün değildir. İştirakin her türlüsünün mümkün olduğu inceleme konumuz olan suç açısından içtima hükümlerinin de uygulanabilmesi mümkün görünmektedir.

ee. Üye İşyerinin Cezai Sorumluluğu:

5464 Sayılı Kanun

Madde 40 - *Bu Kanunun 17'nci maddesinin birinci fıkrasına, 18'inci maddesindeki banka kartı ve kredi kartı ile işlem yapıldığını gösteren işaretleri kaldırma yükümlülüğüne ve 19'uncu maddesinin ikinci fıkrasına aykırı hareket eden üye iş yerlerinin işlerini fiilen yöneten görevli ve ilgili mensupları bin güne kadar adlî para cezası ile cezalandırılırlar.*

Bilindiği gibi sistemin taraflarından biri olan üye iş yerlerinin birtakım yükümlülükleri vardır. Banka Kartları ve Kredi Kartları Kanunu'nun 40. maddesinde de üye işyerlerinin cezai sorumlulukları düzenlenmiştir. Buna göre; Kanun'un 17. maddesinin birinci fıkrasına aykırılık halinde, 18. maddesinin banka kartı veya kredi kartı ile alışveriş yapıldığına ilişkin işaretleri kaldırma yükümlülüğüne aykırılık halinde ve son olarak 19. maddesinin ikinci fıkrasına aykırılık halinde, üye iş yerini fiilen yöneten görevliler veya üye iş yeri çalışanlarının cezalandırılacağı hükme bağlanmıştır. Üye işyerlerinin cezai sorumluluklarının düzenlendiği inceleme konumuz maddede ilk olarak kanunun 17. maddesinin birinci fıkrasına aykırılık cezalandırılmaktadır. Buna

göre, *"Üye işyerleri, kart hamillerinin yapmış oldukları mal ve hizmet alımlarının bedelini banka kartı ya da kredi kartı ile ödeme taleplerini kabul etmek zorundadır. Bu zorunluluk indirim dönemlerinde de geçerlidir. Üye işyerleri, kart hamilinden kartın kullanılması dolayısıyla komisyon veya benzeri bir isim altında ilave bir ödemede bulunmasını isteyemez."* Üye işyerlerinin 40. maddeyle yaptırım altına alınan bir diğer yükümlülüğü ise kanunun 18. maddesinde düzenlenen yükümlülüğüdür. Söyle ki; *"üye işyerleri, banka kartı ve kredi kartı ile işlem yapıldığını gösteren işaretleri, iş yerinin girişinde ve kart hamilleri tarafından kolayca görülebilecek bir yere koymak, üye iş yeri sözleşmeleri herhangi bir nedenle sona erdiği takdirde de, bu işaretleri kaldırmakla yükümlüdür. Üye işyerleri, teknik bir nedenle geçici bir süreyle işlem yapılamadığı hallerde kart hamillerini uyarmakla yükümlüdür."* İnceleme konumuz olan maddede ise; bahse konu bu işaretleri kaldırmamak suç olarak düzenlenmiştir. Son olarak kanunun 19/2 maddesine göre; üye işyerleri kart kullanmak suretiyle satın alınmış bir malın iadesi veya alımından vazgeçilmesi veya işlemin iptal edilmesi durumunda, alacak belgesi düzenlemek ve bir nüshasını kart hamiline verirken bir nüshasını muhafaza etmekle yükümlüdürler. Bu yükümlülüğe aykırı hareket edilmesi halinde de üye iş yerinin cezai sorumluluğu doğar.

Bu suçun mağduru kanunun 17/1 ve 19. maddelerinde düzenlenen eylemlerde kart hamili ve kart çıkaran kuruluş, 18. maddesinde düzenlenen eylemde ise kart çıkaran kuruluş olmaktadır. Bununla beraber, inceleme konumuz olan suç kasten islenebilen bir suç olarak düzenlenmiştir. Esas itibariyle taksirle islenebilmesi mümkün görünse de kanun koyucu buna ilişkin bir düzenleme yapmadığı için kasten islenebildiği sonucuna varılmaktadır. Özel görünüş şekilleri açısından üye işyerlerinin cezai sorumluluğunu düzenleyen suçun iştirak ve içtima hükümleri açısından bir farklılık göstermediğini belirtmek gerekir. Yani iştirak ve içtima hükümlerinin inceleme konumuz olan suçta uygulanabilmesi mümkündür. Bahsi geçen suçla ilgili olarak suçun neticesi harekete bitişik suçlardan olması nedeniyle teşebbüs hükümlerinin uygulanamayacağını belirtmek gerekir.

ff. Denetimde İstenen Bilgi ve Belgeleri Vermemek:

5464 Sayılı Kanun

Madde 41 - *Bu Kanunun 27'nci maddesinin ikinci fıkrası uyarınca istenilen bilgi ve belgeleri vermeyenler ile bu bilgi ve belgeleri gerçeğe aykırı olarak verenler, üç aydan bir yıla kadar hapis ve binbeşyüz güne kadar adlî para cezası ile cezalandırılırlar.*

Banka Kartları ve Kredi Kartları Kanunu 41. maddesinde yine 5411 Sayılı Bankacılık Kanunu'nda 153. maddenin birinci fıkrasında düzenlenmiş olan *"yetkili merciler ile denetim görevlilerince istenen bilgi ve belgeleri vermemek"* suçuna benzer bir suç düzenlenmiştir. Buna göre, aynı Kanun'un 27. maddesinin ikinci fıkrası uyarınca istenilen bilgi ve belgeleri vermeyenler ile bu bilgi ve belgeleri gerçeğe aykırı olarak verenlerin, bu eylemleri yaptırım altına alınmıştır. Yine aynı Kanun'un 4. maddesine istinaden faaliyet izni verilen kuruluşların, faaliyetlerinin denetim ve gözetimi BDDK tarafından sağlanmaktadır. Kanun'un 27. maddesinin ikinci fıkrasında ise; *"Kanun kapsamında yer alan kişi ve kuruluşlar, Kurulca belirlenecek usul ve esaslar çerçevesinde gizli dahi olsa bu Kanunun uygulanması ile ilgili olarak her türlü bilgi ve belgeyi talep üzerine Kuruma tevdi etmekle yükümlüdür."* şeklinde bir yükümlülük düzenlenmiştir. Kanun'un 41. maddesinde *"...bu bilgi ve belgeleri gerçeğe aykırı verenler..."* ifadesiyle ayrıca ikinci bir eylem de yaptırım altına alınmıştır. Buradaki

gerçeğe aykırılık sahtecilik anlamında olmayıp, bahse konu bilgi veya belgenin gerçeğe uymaması, eksik veya fazla olması seklinde anlaşılmalıdır. Zîra kanun koyucu madde metninde sahtecilik sonucuna ulaşılabilecek bir unsurdan bahsetmemiştir. Ancak elbette bahse konu bilgi ve belgelerde sahtecilik yapma ihtimali mevcuttur. Bu durumda sahtecilik suçu da oluşabilecektir. Kurulun istediği ve denetleyeceği tüm bilgi ve belgeler bu suçun konusunu oluştururken, bu bilgi veya belgelerin gizli olmasının bir önemi olmamaktadır. Bu suç, faaliyet izni verilen kuruluşların yönetici veya yetkilileri tarafından işlenebilmektedir. Bu özelliğiyle bu suç özgü bir suçtur. Bununla beraber, bu suçun mağduru veya başka bir deyişle suçtan zarar göreni bilgilerin verilmediği veya yanlış verildiği kurum olarak BDDK'dır. Suçun her iki halde de yani hem vermemek hem de gerçeğe aykırı vermek seklinde gerçeklesen eylemleri açısından kasten islenebilen bir suç olduğunu söylemek gerekir. Esas itibariyle gerçeğe aykırı bilgi veya belge vermek taksirle gerçekleşebilecek olsa da madde metninde açık hüküm bulunmadığından burada suç oluşmayacaktır.

3.3.2. Elektronik İmza Kanunu'nda Yer Alan Suçlar (Eik M. 16-17)

İmza Oluşturma Verilerinin Izinsiz Kullanımı

Madde 16- (Değişik: 23/1/2008 - 5728/525 md.)

Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Elektronik Sertifikalarda Sahtekârlık

Madde 17- (Değişik: 23/1/2008 - 5728/526 md.)

Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."

a. Korunan Hukuksal Değer

Bu suçlar ile korunan hukuksal değer, belgede sahtecilik suçlarıyla korunmak istenilen hukuksal değerle büyük benzerlik göstermektedir. Dolayısıyla devlet tarafından oluşturulan hukuk alanında inandırıcılığı olan bu tür verilere karşı güven ve bunun karşılığı olarak bireylerin de bu verilerin inandırıcılığına ve geçerliliğine olan güvenleri korunmak istenmektedir.[58]

58 Dülger, s.639.

b. Tipikliğin Maddî Unsurları

aa. Fail: Elektronik imza oluşturma verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekarlık yapılması suçlarında fail açısından yasa maddelerinde herhangi bir özellik aranmamıştır. Bu nedenle bu suçları herkes işleyebilecektir. Ancak yasada her iki suç açısından da failin çalıştığı işe bağlı olarak suçun cezasını artırıcı nitelikli hal öngörüldüğü için failin çalıştığı işin tespiti önemlidir. Buna göre eylemi meydana getiren failin elektronik sertifika hizmet sağlayıcısı çalışanı olması durumunda ceza yarısına kadar arttırılarak verilecektir.[59]

bb. Mağdur: Bu suçların mağduru daima toplumdur. Elektronik imza oluşturma verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekârlık yapılması suçları nedeniyle zarara uğrayan kimse mağdur olmayıp "suçtan zarar gören kimse" konumundadır. [60]

cc.Suçların Konusu: Her iki suçun da konusunu genel olarak veriler oluşturmaktadır.Çünkü hem elektronik imzahem de elektronik sertifika sayısal verilerden oluşmaktadır. Ancak bu veriler 5237 sayılı TCK'nın 244. maddesinin konusunu oluşturan verilerden farklı olarak bilişim sisteminde bulunan her türlü veri değil, EİK'da belirtilen elektronik imza ve sertifikanın oluşturulmasında kullanılan verilerdir.

EİK'nın 16. maddesinde belirtilen suçun konusunu elektronik imza oluşturma verileri ve araçları, 17. maddesinde düzenlenen suçun konusunu ise elektronik sertifikalar oluşturmaktadır. Her ne kadar yasal düzenlemede de belirtildiği gibi bunlar farklı araçlar olsa da aslında birbirini tamamlayan ve elektronik imzayı geçerli bir onay sistemi haline getiren araçlardır.[61]

dd. Eylemler:

aaa. Elektronik İmza Oluşturma Verilerinin İzinsiz Kullanımı Suçu Açısından (EİK m.16);

aaaa. Verinin veya Aracın Elde Edilmesi: İmza oluşturma verisinin veya aracının elde edilmesi bir bilişim sistemine girilerek yapılabileceği gibi bunların içinde bulunduğu bir veri taşıma aracının elde edilmesi yoluyla da olabilir. Söz konusu verinin veya aracın elde edilmesi için girilen bilişim sistemine yapılan girişin hukuka aykırı olmasına gerek yoktur. elektronik imza oluşturma verisinin veya aracının elde edilmesi için bunun ilgilisinin açık rızasının olmaması ya da bir başka verinin ya da aracın elde edilmesi için rıza gösterilmesi ancak bu rızanın elektronik imzayı da kapsayıp kapsamadığının açık olmadığı durumlarda bu hareket gerçekleşmiş olacaktır.[62]

bbbb. Verinin veya Aracın Verilmesi: İmza oluşturma verisinin veya aracının verilmesi eylemi de bir bilişim sisteminden veriiletim ağı aracılığıyla yapılabileceği gibi bunların içinde bulunduğu bir veri taşıma aracının

59 Dülger, s.640.
60 Dülger, s.641.
61 Dülger, s.641.
62 Dülger, s.644.

verilmesi yoluyla da gerçekleştirilebilir. Ancak ilgilisinin izni olmadan imza oluşturma verisinin veya aracının verilmesi eyleminin gerçekleştirilebilmesi için öncelikle bunların fail tarafından elde edilmesi gerekmektedir. Ancak bu elde etme eylemi hukuka uygun şekilde gerçekleşebileceği gibi hukuka aykırı olarak da gerçekleşebilir. Verilerin ve araçların verilmesi eyleminin suç oluşturması için öncesindeki elde etme hareketinin hukuksal durumunun önemi olmaksızın, verme hareketinin ilgilinin rızası dışında olması gerekir.[63]

cccc. Verinin veya Aracın Kopyalanması: İmza oluşturma verisinin veya aracının kopyalanması hareketi ise ya veri iletim ağı üzerinden bilişim sistemine girilerek söz konusu veri ya da aracın kopyalanması ya da veri taşıma aracına kopyalama veya bu araçlardan bilişim sistemine kopyalama yapılması yoluyla gerçekleştirilebilir. Yukarıda imza oluşturma verisinin veya aracının verilmesi eyleminde açıklandığı gibi kopyalama eylemine konu olan araç ya da veriler suçu oluşturan eylem öncesinde hukuka uygun olarak ele geçirilmiş olabilir; ancak ilgili kişinin rızası dışında bunun kopyalanması durumunda suçu oluşturan hareket gerçekleşmiş olacaktır.[64]

dddd. İmza Oluşturma Aracının Yeniden Oluşturulması: EİK'nın 3. maddesinin (e) bendinde imza oluşturma aracı tanımlanmıştır. Buna göre "elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı" imza oluşturma aracını oluşturmaktadır. İşte bu aracı oluşturan yazılımın ya da donanımın fail tarafından yeniden oluşturulması inceleme konusu suçu meydana getiren hareketlerden birisi olarak düzenlenmiştir. Buna göre her ne şekilde ve ne amaçla olursa olsun imza oluşturma aracını oluşturan yazılım ya da donanımın ilgilisinin rızası dışında oluşturulması hareketi elektronik imza oluşturma verilerinin izinsiz kullanımı suçunu oluşturacaktır.[65]

eeee. İzinsiz Elektronik İmza Oluşturulması: EİK'nın incelenmekte olan 16. maddesinde izinsiz olarak elde edilen imza oluşturma araçlarının kullanılmasıyla izinsiz elektronik imza oluşturulması da suçu meydana getiren hareketlerden birisi olarak düzenlenmiştir. Buna göre imza oluşturma araçları olan donanımın ve yazılımın fail tarafından izinsiz olarak ele geçirilmesi ve izinsiz olarak elektronik imza oluşturulması hâlinde EİK'nın 16. maddesi ihlal edilmiş olacaktır. Bu ele geçirmenin nasıl gerçekleştiğinin önemi yoktur, önemli olan bunların ilgilinin izni olmaksızın elde edilmesidir. [66]

bbb. Elektronik Sertifikalarda Sahtekarlık Suçu Açısından (EİK m.17);

aaaa. Sahte Elektronik Sertifika Oluşturulması: EİK'nın 3. maddesinin (ı) bendinde elektronik sertifika tanımlanmıştır. Buna göre "imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt" elektronik sertifikayı oluşturmaktadır. İşte bir elektronik sertifikayı oluşturan imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan kaydın kısmen veya tamamen sahte bir şekilde oluşturulması eylemi elektronik sertifikalarda sahtekârlık

63 Dülger, s.645.
64 Dülger, s.645.
65 Dülger, s.645.
66 Dülger, s.646.

suçunu oluşturacaktır.[67]

bbbb. Geçerli Sertifikaların Taklit Edilmesi: *Nitelikleri EİK'nın 8. maddesinde düzenlenen bir elektronik sertifika hizmet sağlayıcısı tarafından oluşturulan geçerli bir elektronik sertifikanın taklit edilmesi hareketi de inceleme konusu suçu meydana getirecektir. Bu taklit hareketi karışık bir algoritmadan oluşan sertifikanın aslına bakılarak yazılması kolay olmadığı için genellikle kopyalama şeklinde olacaktır. Kopyalamanın yapıldığı aracın ise suçun oluşumu açısından önemi yoktur, önemli olan sonuçta geçerli olan sertifikayla aynı özelliklere sahip ve aynı sonuçları doğuracak bir taklit sertifikanın oluşmasıdır.*[68]

cccc. Geçerli Sertifikaların Tahrif Edilmesi: Tahrif etmek sözcüğünün anlamı TDK'nın elektronik sözlüğünde "bozmak, değiştirmek" olarak açıklanmaktadır. Geçerli bir elektronik sertifikanın her ne şekilde olursa olsun fail tarafından değiştirilmesi ya da bozulması hareketiyle EİK'nın 17. maddesi ihlal edilmiş olacaktır. Bu değiştirme ya da bozma hareketi sertifikayı oluşturan verilere yeni veriler eklenmesi ya da var olan verilerin çıkarılması yoluyla olabileceği gibi mevcut verilerin yerlerinin değiştirilmesi yoluyla da olabilecektir. Ancak verilerde değiştirme yapılmak suretiyle kısmen veya tamamen sahte bir sertifika oluşturulması halinde artık tahrif etme hareketi gerçekleşmemekte, sahte elektronik sertifika oluşturulması hareketi gerçekleşmiş olmaktadır.[69]

dddd. Sahte Sertifika Kullanılması: EİK'nın 17. maddesinde, yukarıda anılan sahte, taklit, tahrif edilmiş ya da yetkisiz olarak oluşturulmuş elektronik sertifikaların bilerek kullanılması hareketi düzenlenmiştir. Söz konusu kullanmak hareketinin hukuk alanında delil olarak kullanılması gerekli değildir. Her ne amaçla kullanılırsa kullanılsın bu suçun oluşması açısından gerekli olan, söz konusu sertifikanın sahte olduğunun bilinerek kullanılmasıdır.

Failin kendi oluşturduğu sahte sertifikayı kullanmasının suçun oluşumu açısından her hangi bir özelliği yoktur. Tek suç tipi içinde hem sertifikanın oluşturulması hem de oluşturulan sertifikanın kullanılması, suçu oluşturan seçimlik hareketler olarak düzenlendikleri için suçun oluşumunu etkilememektedir. [70]

ee. Suçun Nitelikli Hâli: EİK'nın 16. ve 17. maddelerinin 2. fıkralarında her iki suç için de aynı ağırlatıcı nitelikli hal öngörülmüştür. Buna göre "yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar arttırılır" denilmek suretiyle fail açısından elektronik hizmet sağlayıcısı çalışanı olunması durumu, cezanın yarısına kadar arttırılmasını gerektirecektir.[71]

c. Tipikliğin Manevî Unsuru

EİK'nın 16. maddesinde düzenlenen suç açısından yasa koyucu, failin eylemlerini "elektronik imza oluşturma amacıyla" yapmasını aramıştır. Böylece suçun oluşumu için failde suç işleme kastının yanında ayrıca amaç unsurunun da bulunması

67 Dülger, s.647.
68 Dülger, s.648.
69 Dülger, s.648.
70 Dülger, s.648.
71 Dülger, s.649.

gerekir. Failin eylemlerini "elektronik imza oluşturma amacıyla" gerçekleştirmemesi durumunda eğer eylemleri diğer bir suçu oluşturuyorsa bu maddelerden dolayı cezalandırılacak, eğer başka suç oluşturmuyorsa faile ceza verilmeyecektir.

EİK'nın 17. maddesinde düzenlenen suç açısından ise yasa koyucu failin eylemlerini kasten gerçekleştirmesini aramıştır. Failin 16. maddede düzenlenen suç tipinden farklı olarak belli bir amaçla hareket etmesi aranmadığı için söz konusu suçun manevî unsuru yalnızca kasttır.[72]

d. Hukuka Aykırılık Unsuru

Failin EİK'nın 16. maddesinde düzenlenen suçu oluşturan eylemleri bir elektronik imza ile ilgili kişinin iznine dayanarak gerçekleştirdiği hallerde suç oluşmayacaktır, çünkü maddede suçun oluşması için failin, ilgilinin izni olmadan eylemlerini yapması aranmıştır, rızanın varlığı hâlinde bu hukuka aykırılıkortadan kalkacaktır. Ancak yasada bu ilgili kişinin kim olduğu konusunda açıklık bulunmamaktadır. Bu kişinin elektronik imzanın kullanılması açısından hak sahibi olan kişi olması yasanın genel düzenlemesine uygundur. Hak sahipliğine bağlı olarak imza üzerinde kullanım yetkisi olan kişi rızayı vermeye de yetkili olan kişidir.

EİK'nın 17. maddesi açısından ise ne ilgilinin rızasından kaynaklanan ne de yasadan kaynaklanan bir hukuka uygunluk sebebi bulunmaktadır.[73]

e. Suçun Özel Görünüş Biçimleri

aa. Teşebbüs: EİK'in 16. ve 17. maddelerinde düzenlenen suçlar yukarıda da belirtildiği üzere hareket dışında ayrıca neticenin aranmadığı, sırf hareket suçlarıdır. Bu nedenle bu suçlara teşebbüs ancak eylem unsurunu oluşturan hareketlerin parçalara bölünebilmesi halinde söz konusu olabilecektir. Ancak failin elinde olmayan nedenlerden ötürü yasada belirtilen suçun işleniş şekillerinin örneğin elektrik kesilmesi ya da sistemin kapatılması gibi bir nedenle yarıda kalması gibi durumlarda suç teşebbüs aşamasında kalabilecektir.[74]

bb. İştirak: EİK'in 16. ve 17. maddelerinde düzenlenen suçlarda iştirak açısından bir özellik söz konusu olmayıp, ortaya çıkacak iştirak halleri TCK'nın 37, 38, 39, 40 ve 41. maddelerine göre değerlendirilecek ve ortaya çıkacak sorunlar çözülecektir.[75]

cc. İçtima: EİK'in 16. maddesinde düzenlenen imza oluşturma verilerinin izinsiz kullanımısuçunun, TCK'nın 244/1-2. maddesinde düzenlenen "Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması Suçu ile Verilerin Yok Edilmesi veya Değiştirilmesi Suçu", 244/4'te düzenlenen "Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu", 135. maddede düzenlenen "Kişisel Verilerin Kaydedilmesi Suçu" ve 136. maddede düzenlenen "Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu" ile içtima hâlinde bulunması mümkündür.

Ancak EİK yalnızca elektronik imzayla ilgili düzenlenmiş bir yasa olduğu için

72 Dülger, s.650.
73 Dülger, s.651.
74 Dülger, s.651.
75 Dülger, s.651.

içerdiği suç tipleri de özel olarak elektronik imzayla ilgilidir. Her ne kadar elektronik imzalar da verilerden oluşmakta ve bunlar üzerinde gerçekleştirilen eylemler yukarıda anılan TCK'da düzenlenen suç tiplerini de ihlal eder nitelikte olsalar da, EİK'nın TCK karşısında özel bir yasa olması nedeniyle EİK'da düzenlenen ceza normları da TCK'nın ceza normlarına göre özel hükümniteliğindedir. Bu nedenle EİK'in 16. maddesinin TCK'da düzenlenen bilişimsuçlarıyla içtima ilişkisinde bulunması durumunda EİK'in 16. maddesi uygulama alanı bulacaktır. Dolayısıyla EİK, TCK karşısında da özel yasa niteliğinde olduğu için çıkabilecek içtima sorunları özel hüküm – genel hükümilişkisi çerçevesinde çözülecektir.

EİK'in 17. maddesinde düzenlenen elektronik sertifikalarda sahtekârlık suçunun diğer bilişim suçlarıyla içtima halinde olması halinde de yukarıda belirttiğimiz üzere EİK'in özel yasa olması nedeniyle "genel hükümler" dışında kalan suç tiplerine ilişkin düzenlemelerde öncelikle bu yasada yer alan suç normları uygulama yeri bulacaktır.[76]

f. Yaptırım, Soruşturma ve Kovuşturma

EİK'in 16. ve 17. maddelerinde düzenlenen suçları işleyen failler için hem hürriyeti bağlayıcı ceza hem de Adlî para cezası öngörülmüştür. Yasa'nın 16. maddesinde yer alan suç için bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezası öngörülmüştür. Yasa'nın 17. maddesinde yer alan suç için ise iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezası öngörülmüştür. TCK'nın 52. maddesinde adlî para cezasının yasada aksine bir hüküm bulunmaması halinde yedi yüz otuz günden fazla olamayacağı belirtildiği için adlî para cezasının gün sayısının tespitinde üst sınır olarak bu sayı esas alınacaktır.[77]

3.3.3. Online Kumar (TCK 228)

Online Kumar (TCK 228); Her ne kadar Afyon'daki seminer sırasında online kumardan bahsedilirken TCK 228 maddesine atıfta bulunulmuş ise de aşağıdaki yasal metninden de anlaşılacağı üzere bu maddenin normal kumar oyunlarında yer temin edeni cezalandırdığı aşikardır. Normal kumar oynama eylemi ise suç ve ceza kapsamında değil, kabahat kapsamında ve 5326 sayılı kabahatler kanununun 34. maddesine göre idari yaptırımla cezalandırılmıştır.

a-Kumar Oynanması Için Yer ve İmkân Sağlama TCK Madde 228

(1) Kumar oynanması için yer ve imkân sağlayan kişi, bir yıla kadar hapis ve adlî para cezası ile cezalandırılır.

(2) Çocukların kumar oynaması için yer ve imkân sağlanması hâlinde verilecek ceza bir katı oranında artırılır.

(3) Bu suçtan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

(4) Ceza Kanununun uygulanmasında kumar, kazanç amacıyla icra edilen ve kar ve zararın talihe bağlı olduğu oyunlardır

b-5326 Sayılı Kabahatler Kanunu Madde 34

76 Dülger, s.651.

77 Dülger, s.651.

(1) Kumar oynayan kişiye, yüz Türk Lirası idari para cezası verilir. Ayrıca, kumardan elde edilen gelire elkonularak mülkiyetin kamuya geçirilmesine karar verilir.
(2) Bu kabahat dolayısıyla idari para cezasına ve elkoymaya kolluk görevlileri, mülkiyetin kamuya geçirilmesine mülki amir karar verir.

c-Online kumar ise özel olarak 7258 sayılı yasa düzenlenmiştir. 7258 sayılı Futbol Ve Diğer Spor Müsabakalarinda Bahis Ve Şans Oyunlari Düzenlenmesi Hakkında Kanun'un 5.maddesinde, *'Kanunun verdiği yetkiye dayalı olmaksızın, spor müsabakaları ile ilişkili olarak sabit ihtimalli veya müşterek bahis oynatanlar, oynanmasına yer veya imkân sağlayanlar, bir yıldan üç yıla kadar hapis ve onbin güne kadar adlî para cezasıyla cezalandırılır.Yurt dışında oynatılan her çeşit bahisveya şans oyunlarının internet yoluyla ve sair suretle erişim sağlayarak Türkiye'den oynanmasına imkân sağlayan kişiler, iki yıldan beş yıla kadar hapis cezasıyla cezalandırılır.Her türlü bahis veya şans oyunlarıyla bağlantılı olarak para nakline aracılık eden kişiler, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezasıyla cezalandırılır. Kişileri, reklam vermek ve sair surette, her türlü bahis veya şans oyunlarını oynamaya teşvik edenler, altı aydan iki yıla kadar hapis ve üçbin güne kadar adlî para cezasıyla cezalandırılır.Bu maddede tanımlanan suçlarla bağlantılı olarak, her türlü bahis veya şans oyunlarının oynanmasına tahsis edilen veya oynanmasında kullanılan ya da suçun konusunu oluşturan eşya ile bu oyunların oynanması için ortaya konulan veya oynanması suretiyle elde edilen her türlü mal varlığı değeri, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun eşya ve kazanç müsaderesine ilişkin hükümlerine göre müsadere edilir.Bu maddede tanımlanan suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.Bu maddede tanımlanan suçlarla ilgili olarak, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun erişimin engellenmesine ilişkin hükümleri uygulanır.'* şeklinde özel bir düzenlemeye yer verilmiştir. Ayrıca 21/5/1986 tarihli ve 3289 sayılı Gençlik ve Spor Genel Müdürlüğünün Teşkilat ve Görevleri Hakkında Kanunun 10 uncu maddesi ile 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun hükümlerine dayanılarak spor **müsabakalarina dayalı sabit ihtimalli ve müşterek bahis oyunlari uygulama yönetmeliği** 28.02.2009 tarihli Resmî Gazete'de yayınlanmıştır.

3.3.4. Çocuk Pornografisi (TCK 226/3)

"...(3) Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır."

Kanun'un üçüncü fıkrasında, müstehcenliğe karşı çocukları korumaya yönelik iki ayrı suç tanımına yer verildiği görülmektedir. Bunlardan birincisi; müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların kullanılması suretiyle oluşmaktadır. İkinci suç ise, bu ürünlerin ülkeye sokulması, çoğaltılması, satışa arzı, satışı, nakli, depolanması, ihracı, bulundurulması ya da başkalarının kullanımına sunulması fiillerinden birinin işlenmesiyle oluşmaktadır. Yani, maddenin üçüncü fıkrası ile çocuk pornosu suç haline getirilerek, çocukların müstehcen ürünlerin üretiminde kullanılması ve çocukların kullanıldığı müstehcen ürünlerin ülkeye sokulması,

çoğaltılması, satışa arz edilmesi, satılması, nakledilmesi, depolanması, ihraç edilmesi, bulundurulması ya da başkalarının kullanımına sunulması bu suç kapsamına alınmıştır. TCK'mn 226/3. maddesiyle, çocuk pornosu tabiri kullanılmadan müstehcen içerikteki ürünlerin üretiminde, meydana getirilmesinde çocukların kullanılması suç olarak düzenlenmiştir. Burada geçen müstehcen ürün tabiri ile anlatılmak istenen çocuk pornografisidir.

Çocuk pornosunda dikkate edilmesi gereken husus, suça konu olan nesnenin, görüntü, yazı veya söz içermesidir. Yani bu tür özelliğine sahip olmayan örneğin, tahrik edici bir koku bu suçun konusu olmayacaktır.

Çocuk pornosonu içeren görüntü, ses veya sözlerin genellikle bilişim sistemleri vasıtasıyla işlendiği görülmektedir. Örneğin, yurt dışı kaynaklı bir internet sitesi üzerinden bu tür görüntünün mail yoluyla bilgisayarınıza gönderilmesi, sosyal paylaşım sitelerinden olan facebook.com adresi üzerinden bu tür bir görüntü veya ses kaydının paylaşılması, sanal ortamdan bu tür görüntülerin satılması, sanal ortamda görüntülerin oynatılması, sanal ortamda bu tür filmlerin arşivlenerek depo edilmesine uygulamada sıkça rastanılmaktadır.

Bu suçla (çocuk pornosu) korunan hukukî yarar, çocukların bedensel, zihinsel, ahlâkahlâkî, ruhsal ve duygusal tamlığının korunması olduğu kadar, çocukların psikolojik yapılarının zarar görmesinin önlenmesidir. Cinsel istismarın bir türü olan çocuk pornografisinin cezalandırma konusu olması,çocuğun ruhsal ve fiziksel gelişimini henüz tamamlamamış olması ve onun kendi cinsel davranışı üzerinde özerk bir karar verme yeteneğinin henüz gelişmemiş olmasından kaynaklanmasındandır.
Üçüncü fıkrada düzenlenen suçun mağduru 18 yaşını tamamlamamış kimseler olan çocuklardır. 18 yaşını doldurmamış, ancak resmi olarak evlenmiş kimseler, suçun mağduru olamayacaktır. Müstehcen ürünün konusunun gerçek bir çocuk olması şart değildir, burada önemli olan ürünün algısal içeriğidir.

Pornografik görüntü konusunda bir çok tanım yapılsa da, çocuk haklarını korumaya yönelik Birleşmiş Milletler tarafından oluşturulan Çocuk Hakları Sözleşmesi'ne üye devletler arasında 25.05.2000'de imzalan 4755 sayılı Yasa ile uygun bulunarak kabul edilen Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi ile İlgili İhtiyari Protokolün 2. maddesinin c bendinde çocuk pornosu tanımlanmıştır. Buna göre çocuk pornografisi, *"Çocuğun gerçekte veya taklit suretiyle bariz cinsel faaliyetlerde bulunur şekilde herhangi bir yolla teşhir edilmesi veya çocuğun cinsel uzuvlarının, ağırlıklı olarak cinsel amaç güden bir şekilde gösterilmesidir."* şeklinde tanımlanmıştır. Bir eserin pornografik sayılabilmesi için, bir bütün olarak objektif açıdan önemli ölçüde cinsel dürtüleri tahriki amaçlaması, insani ilişkilere yer vermemesi, insanı cinsel bir obje haline indirgemiş olması, daha açık bir deyişle cinselliği mutlak hale getirmiş olması, cinsel davranışları estetikten uzak, tahrike yönelik bir şekilde ve sadece ayrıntılı bir biçimde cinsel organları göstermesi gerekir. Bu özellikleri kendinde toplayan eser pornografik bir eserdir. (Özbek, Müstehcenlik Suçu, (2009), sh. 19-21, Aktaran, Osman Yaşar, Mustafa Artuç, TCK Yorumu)

Avrupa Konseyi Siber Suç Sözleşmesi'nin 9. maddesine göre, çocuk pornografisi kavramı,

a) cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı

b) cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı
c) cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren gerçeğe benzer görüntüleri ifade etmektedir.

Çocuk Haklarına Dair Birleşmiş Milletler Sözleşmesi'nin 32.maddesine göre, taraf devletler, çocuğun bedensel, zihinsel, ruhsal, ahlâkahlâkî ya da toplumsal gelişmesine zararlı olabilecek nitelikte çalıştırılmasına karşı koruma sağlayacaktır. Bu sözleşmenin 34.maddesine göre ise,

a) çocuğun yasadışı bir cinsel faaliyete girişmek üzere kandırılması veya zorlanmasını,
b) çocukların fuhuş ya da diğer yasadışı cinsel faaliyette bulundurularak sömürülmesini,
c) çocukların pornografik nitelikteki gösterilerde ve malzemede kullanılmasını önlemek amacıyla ulusal ve ulusal arası düzeyde gerekli her türlü önlemi alacaklardır.

TCK'nın 226. maddesi uyarınca müstehcen yayın yapıldığının kesin olduğu durumlarda bilirkişiye gitmeye gerek olmamakla birlikte bazı hadiselerde uygulamayı yapacak olan kişiler tereddüde düşebilirler, işte bu gibi durumlarda 1117 sayılı Küçükleri Muzır Neşriyattan Koruma Kanunu hükümlerine göre resmi bilirkişilik yapmakla görevlendirilen Başbakanlık Küçükleri Muzır Neşriyattan Koruma Kurulu'na müracaat edilebilecektir. Ya da, müstehcen olduğu ileri sürülen eserin bilimsel bir eser, sanatsal veya edebî değeri olan bir eser olma ihtimali olduğunda, bu konuda üniversiteden seçilecek hukukçu bilirkişiler aracılığıyla bilirkişi incelemesi yaptırılması da mümkündür. Yargıtay bu konuda ehil olmayan kişilerin verdiği raporların karara esas alınamayacağını belirtmektedir. Yargıtay 5.CD'nin 05.02.2007 tarih ve 2006/13422-2007/757 sayılı kararında *"...Dava konusu filmin içeriğinin halkın ar ve haya duygularını incitir veya cinsi arzularını tahrik ve istismar eder nitelikte genel ahlâka aykırı olup olmadığı, ürün üretiminde çocukların kullanılıp kullanılmadığı bilirkişi incelemesi yaptırılarak saptanmadan söz konusu yabancı filmin genel ahlâk ve adaba aykırı, pornografik içerikli olduğunu belirten polislerce düzenlenen tutanağa dayanılarak yazılı şekilde karar verilmesi "* bozma sebebi sayılmıştır.

Maddenin üçüncü fıkrasında düzenlenen suçun hareket unsuru, müstehcen görüntü, yazı ve sözleri içeren ürünlerin üretiminde çocukları kullanmak, çocukların kullanıldığı ürünleri, ülkeye sokmak, çoğaltmak, satışa arz etmek, satmak, nakletmek, depolamak, ihraç etmek, bulundurmak ve başkalarının kullanımına sunmaktır. Burada dikkate edilmesi gereken, suçun işlenmesi için ticari amaç şartının bulunmamasıdır. Yani, kişisel ihtiyaç örneğin zevk için, müstehcen görüntülerin maddede belirtilen seçimlik hareketlere konu edilmesi durumunda suç oluşacaktır. Yargıtay 5. CD nin 5.CD'nin 01.10.2007 tarih ve 2007/9856-2007/6957 sayılı kararına göre, *"kasıtlı olarak yapılan bireysel amaçlı bulundurma ve depolamanın da suç sayıldığı, bu nedenle sanığın oluşa uygun olarak işlediği kabul edilen ve müstehcen görüntülerin miktarına, niteliğine ve kayıt biçimine göre uzun süre içerisinde ve kasten yapıldığı anlaşılan çocuk pornografisi ve hayvanlarla yapılan cinsel davranışlara ilişkin çok sayıda resim ve video kaydını bilgisayar sistemi vasıtasıyla temin edip bilgisayarında sistematik biçimde depolama ve bulundurma"* fiilinin kişisel amaçlı dahi olsa *5237* sayılı TCK. nın 44.maddesi yoluyla aynı yasanın 226/3. maddesine uyan suçu oluşturduğu belirtilmektedir.

Maddede geçen üretmek tabirinden, müstehcen nitelikteki görüntü, yazı ve

sözlerin meydana getirilmesi anlaşılmalıdır. Yani, pornografik filmin çekilmesinden sonra CD'nin depolanmasında çocuğun kullanılması suçun oluşumuna sebebiyet vermeyecektir.

TCK'nın 226/3. maddesinde düzenlenen suç seçimli hareketli bir suçtur.Bu nedenle eylemin anılan suçu oluşturması için maddede sayılan hareketlerden birisinin yapılması gerekir. Bu eylemlerden hepsinin yapılması ile değil, yalnız birisinin yapılması ile anılan suç oluşacaktır.

Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların kullanıldığı sırada, çocuklara karşı cinsel istismar suçu da işlenmekte ise,TCK'nın 44. maddesinden düzenlenen fikri içtima hükümlerinin uygulanması gerekecektir. Bu durumda TCK'nın 103/2. maddesi hükmünde öngörülen ceza daha ağır ceza hükümleri içerdiğinden TCK nın 226/3. maddesi değil, TCK nın 103/2. maddesi gereğince ceza verilecektir.

3.3.5. Haberleşmenin Engellenmesi (TCK 124)

"Madde 124

(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hâlinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi hâlinde, ikinci fıkra hükmüne göre cezaya hükmolunur."

5237 sayılı TCK'nın İkinci Kitabı'nın *"Kişilere karşı suçlar"* başlıklı İkinci Kısmı'nın *"Hürriyete karşı suçlar"* başlıklı Yedinci Bölümü'nün 124. maddesinde düzenlenen *"haberleşmenin engellenmesi suçu"*, her türlü iletişim aracıyla yapılan haberleşmeyi kapsamakta ve dolayısıyla bilişim sistemleri aracılığıyla yapılan iletişimi de içermektedir.

Günümüzde gerçekleştirilen haberleşmenin büyük bir çoğunluğunu elektronik posta ve sohbet oluşturmaktadır. Bu yöntem diğerlerine göre hem daha ucuz hem de çok daha hızlı olması nedeniyle artık daha çok tercih edilir hale gelmiştir. Bunların yanı sıra, veri iletim ağları üzerinden yapılan telefon görüşmeleri ve tele-konferanslar da elektronik haberleşmenin diğer çeşitleri olarak görülmektedir.

TCK'nın inceleme konusu maddesinde yalnızca haberleşme denildiği, bu haberleşme araçları tek tek sayılmadığı için haberleşme hangi araçla gerçekleştirilirse gerçekleştirilsin bunun engellenmesi inceleme konusu suçu oluşturacaktır, nitekim bu durum maddenin gerekçesinde de açıkça ifade edilmiştir. Bu nedenle bilişimsistemleri aracılığıyla gerçekleştirilen haberleşmenin engellenmesi eylemleri de TCK'nın 124. maddesinde düzenlenen suç tipinin koruma kapsamında değerlendirilecektir.

Bilişim sistemleri üzerinden yapılan haberleşmenin engellenmesi amacıyla bilişim sistemine veya sistemde yer alan verilere zarar verilmesi halinde ise failin tek eylemiyle yasanın birden fazla suç normu ihlal edilmiş olacağı için düşünsel birleşme kuralı uygulanarak cezası daha fazla olan suçun cezası faile verilecektir. Bu durumda failin kişiler arasındaki haberleşmeyi engellemek amacıyla bu eylemi gerçekleştirmesi halinde TCK'nın 244/1-2. maddesinde düzenlenen bilişim sistemine ve verilere zarar

vermek suçu uygulanacaktır. Failin 124. maddenin 2. fıkrasında düzenlenen kamu kurumları arasındaki haberleşmeyi engellemek amacıyla eylemini gerçekleştirmesi halinde ise, bu suçun cezası 244/1-2'ye göre daha fazla olduğu için faile 124/2. madde uygulanacaktır.[78]

3.3.6. Özel Hayata Ve Hayatın Gizli Alanına Karşı İşlenen Suçlar/Kişisel Verilere Karşı Suçlar (TCK 132,133,134,135,136,137,138)

3.3.6.1. Haberleşmenin Gizliliğini İhlal Suçu (m.132)

"(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse,bir yıldan üç yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat arttırılır.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis veya adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."

TCK'nın 132. maddesinin 1. fıkrasında, kişiler arasındaki haberleşmenin gizliliğinin ihlal edilmesi suç hâline getirilmiştir. Bu eylem sırasında haberleşme içeriğinin kayıt edilmesi de bu fıkranın ikinci tümcesinde suçun nitelikli hali olarak düzenlenmiştir. Bu suç haberleşmenin tarafı olmayan kişi tarafından işlenebilir. Bu suçta "mağdurların çokluğu" suçun tanımında yer alan bir unsur niteliğindedir.

Maddenin 2. fıkrasında ise, kişiler arasındaki haberleşmenin üçüncü bir kişi tarafından açıklanması eylemi suç hâline getirilmiştir. Kişinin kendisi tarafından yapılan haberleşmenin bu haberleşmeyi yapan diğer tarafın izni olmaksızın açıklanması da maddenin 3. fıkrasında suç hâline getirilmiştir. Bu haberleşmenin basınve yayın yoluyla açıklanması da 4. fıkrada cezayı artıran nitelikli hâl olarak öngörülmüştür.

Madde metninde görüldüğü gibi TCK'nın 195. maddesinde düzenlenen posta ve telefon haberleşmesinin gizliliği suçundan farklı olarak bu maddede yalnızca "haberleşme" kavramı kullanılmış; ancak bunun nasıl gerçekleştirildiği belirtilmemiştir. O hâlde her türlü haberleşme bu maddenin koruması kapsamındadır.

Günümüzde gelişen teknoloji sayesinde bilişim sistemleri kullanılarak özellikle de internet aracılığıyla elektronik posta, elektronik sohbet (chat), internet üzerinden telefon görüşmesi ya da tele-konferans gibi çeşitli yöntemlerle haberleşme sağlanmaktadır. İşte bilişim sistemi aracılığıyla gerçekleştirilen bu yeni haberleşme yöntemleri de TCK'nın söz konusu maddesinin düzenlemesiyle koruma altına alınmakta ve bu tür haberleşmeyi ihlal edenler de cezalandırılmak istenmektedir. Bu durum maddenin gerekçesinde de açıkça belirtilmiştir.[79]

3.3.6.2. Kişiler Arasındaki Konuşmaların Dinlenmesi veya Kayda Alınması Suçu (m.133)

"(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin

78 Dülger, s.607.

79 Dülger, s.610.

rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi,iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(3) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."

Bu suçta ise, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suç haline getirilmiştir. Özellikle günümüzde cep telefonlarının aynı zamanda ses ve görüntü kaydetme işlevlerinin olması, öte yandan ses ve görüntü kaydetmek için üretilen araçların son derece küçülmesi bu tür eylemlerin sıklıkla gerçekleştirilmesine yol açmaktadır.

Maddenin 1. fıkrasında kişiler arasında aleni olmayan konuşmaların taraflardan herhangi birinin rızası olmaksızın bir aletle dinlenmesi veya bunların ses alma cihazıyla kaydedilmesi suç haline getirilmiştir.

Maddenin 2. fıkrasında ise kişinin kendisinin de katıldığı aleni olmayan bir söyleşiyi ses alma cihazıyla kaydetmesi suç haline getirilmiştir.

Maddenin 3. fıkrasında ise 1. ve 2. fıkralarda düzenlenen suçların işlenmesi suretiyle elde edilen bilgilerden, failin bilgilerin bu özelliğini bilerek yarar sağlaması veya bunları başkasına vermesi veya diğer kişilerin bilgi edinmesi sağlaması halleri suç olarak düzenlenmiştir. Ayrıca bu konuşmaların basın ve yayın yoluyla yayınlanması halinde de aynı cezanın verileceği belirtilmiştir. Bize göre failin 1. veya 2. fıkradaki suçu işledikten sonra 3. fıkradaki suçu işlemesi halinde her iki suçtan da ayrı ayrı cezalandırılması gerekir. Zîra konuşmaları dinlemek ve kayda almak sonucunda bunların mutlaka açıklanması, başkasına verilmesi ya da bundan bir yarar sağlanması gerekmemektedir. Ayrıca 3. fıkradaki suçun işlenmesi için failin mutlaka 1. veya 2. fıkradaki suçları işlemesi gerekmediği için bunların cezalandırılmayan önceki hareketler olarak kabul edilmeleri de mümkün değildir.[80]

3.3.6.3. Özel Hayatın Gizliliğini İhlal Suçu (m.134)

"(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse,bir yıldan üç yıla kadar hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat arttırılır.

(2)Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."

Özel hayatın gizliliğini ihlal suçu da son zamanlarda sıklıkla karşılaşılan ve bazı eylemler nedeniyle basında da geniş yer tutan bir suçtur. 134. maddedeki bu düzenleme 5237 sayılı TCK ile ceza hukuku mevzuatına yeni getirilmiş bir suç olup Anayasa'nın 20. maddesindeki kişinin özel hayatının ve aile hayatının gizliliğini korumayı amaçlamaktadır.

80 Dülger, s.610.

134. maddenin yer aldığı bölümün başlığı "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" olarak düzenlenmiştir. Bölüm içinde yer alan diğer suçlara da bakıldığında 132, 133, 135, 136 ve 138. maddelerde bir şekilde özel hayatın gizliliğine ilişkin bilgi ve verilerin korunmaya çalışıldığı görülmektedir. 134. madde de ayrıntılı bir tanımlama yapılmaksızın "özel hayatın gizliliğini ihlal eden kimse" denilmek suretiyle suç tanımlanmıştır. Buna göre 134. maddede yer alan suç, diğerlerine göre genel nitelikte olup, bu bölümde yer alan diğer maddelerin uygulanamadığı hallerde 134. maddenin uygulama alanı bulması gerekir.

134. maddenin 1. fıkrasının 1. tümcesinde suç tipi herhangi bir tanımlama yapılmaksızın, serbest hareketli olarak düzenlenmiştir. Dolayısıyla kişinin özel yaşamının gizliliğini ihlal edebilecek her türlü eylemle bu suçun işlenmesi mümkün olacaktır.

134. maddenin 1. fıkrasının 2. tümcesinde ise özel hayatın gizliliğinin görüntü veya seslerin kayda alınması suretiyle işlenmesi suçun nitelikli hâli olarak düzenlenmiş ve cezasının alt sınırının bir yıldan az olamayacağı belirtilmiştir.

134. maddenin 2. fıkrasında ise, kişilerin özel hayatına ilişkin görüntü ve seslerin ifşa edilmesi ayrı bir suç olarak düzenlenmiştir. Ayrıca bu suçun basın ve yayın yoluyla işlenmesi suçun nitelikli hâli olarak düzenlenmiş ve suçun temel hâline göre cezanın yarı oranında artırılacağı belirtilmiştir.[81]

3.3.6.4. Kişisel Verilerin Kaydedilmesi

95/46 sayılı AB Veri Koruma Direktifi'nde kişisel veri, " doğrudan ya da dolaylı olarak gerçek kişi ile ilintili olabilecek ve onu belirlenebilir kılacak her türlü bilgi" olarak tanımlanmıştır.

"(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlâkahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."

a. Korunan Hukuksal Değer

TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu; TCK'nın "Özel hükümler" başlıklı İkinci Kitabı'nın, "Kişilere karşı suçlar" başlıklı İkinci Kısmı'nın, "Özel hayata ve hayatın gizli alanına karşı suçlar" başlıklı dokuzuncu bölümünde düzenlenmektedir. Yasanın sistematiğinden de açıkça anlaşıldığı üzere bu suç tipiyle genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özel olarak ise kişisel veriler korunmaktadır.[82]

b.Tipikliğin Maddî Unsurları

aa. Fail: Madde metninde suçu işleyecek kişi açısından "kimse" sözcüğü kullanılarak bunun dışında herhangi bir özellik belirtilmemiştir; bu nedenle bu suçun faili herkes olabilir. Dolayısıyla kişisel verilerin kaydedilmesi suçu, fail açısından bir özellik göstermemektedir.[83]

81 Dülger, s.611.

82 Dülger, s.561.

83 Dülger, s.563.

bb. Mağdur: Kişisel verilerin kaydedilmesi suçunda tüm gerçek kişiler suçun mağduru olabilir, suç tipi bu açıdan bir özellik göstermemektedir. Ancak suçun mağduru ancak gerçek kişiler olabilecektir. Tüzel kişilerin suç mağduru olmasının suç teorisi bakımından mümkün olmaması dolayısıyla tüzel kişlerin verileri aleyhinde yapılacak benzer eylemlerde şartları varsa tüzel kişiliğin yetkilisi gerçek kişiler suçun mağduru olacaktır. Bunun dışında ticari şirketlerin, ticari sırlarına yönelik benzer eylemler ancak şartları oluşması halinde TCK m.239'da düzenlenen ticari sırların açıklanması suçunu oluşturabilir.[84]

Bu suçun mağduru olmak için mutlaka bilişim sistemine kaydedilen verilerin maliki veya zilyedi olunması gerekmemektedir; önemli olan kaydedilen kişisel verilerin bireyle ilgili olmasıdır.

cc. Suçun Konusu: TCK'nın 135. maddesinde düzenlenen bu suçun konusunu *"kişisel veriler"* oluşturmaktadır. Ayrıca bu maddenin 2. fıkrasında *"kişilerin siyasal, felsefi ve dinsel görüşlerine, ırksal kökenlerine, sendikal bağlantılarına, cinsel yaşamlarına ve sağlık durumlarına ilişkin kişisel verilerin"* de suçun konusunu oluşturduğu ayrıca belirtilmiştir.

Burada tekrar vurgulanması gerekir ki, bu bilgilerin bir bilişim sisteminde kullanılabilecek ve aktarılabilecek şekilde veri hâlinde olması şart değildir; çünkü maddenin gerekçesinde *"verilerin sanal ortamda ya da somut kağıt üzerinde kayda alınması açısından fark gözetilmediği"* belirtilmiştir. Yani bu suç tipinde veri kavramı dar anlamda *"bir bilişim sisteminde ya da veri taşıma aracında bulunan ve üzerinde işlem yapılan sayısal kod halinde bilgi"* olarak değil geniş anlamda *"her türlü bilgi"* olarak kullanılmıştır.[85]

dd. Eylem: Bu suç tipiyle her türlü kişisel verinin bilişim sistemlerine ya da yazılı kayıtlara hukuka aykırı olarak yerleştirilmesi suç hâline getirilmiştir. Verilerin sanal ortamda ya da kağıt üzerinde kayda alınması açısından fark gözetilmediği maddenin gerekçesinde de belirtilmiştir. Buna göre verilerin kaydedilmesi bir bilişim sistemine ya da veri taşıma aracına sayısal kod hâlindeki dar anlamda verilerin girilmesi şeklinde olabileceği gibi, kişisel bilgilerin bir dosya kâğıdına el yazısı ya da daktilo ile geçirilmesi şeklinde de olabilecektir.

c. Tipikliğin Manevî Unsuru

Bu suç kast ile işlenebilir. Suç normunda manevi unsur açısından başkaca bir özellik aranmamıştır. Suçun işlenmesi için failin kastla hareket etmesi gerektiği ve bu konuda başka bir özellik belirtilmemesi nedeniyle bu suçun taksirle işlenmesi mümkün değildir.[86]

d. Suçun Nitelikli Hâlleri

TCK'nın 137. maddesinde *"nitelikli hâller"* başlığı altında özel hayata ve hayatın gizli alanına karşı suçlar bölümünde yer alan suçlar için failin sıfatından kaynaklanan cezayı artırıcı nitelikli haller öngörülmüştür. Buna göre:

84 Dülger, s.563.
85 Dülger, s.564.
86 Dülger, s.566.

"Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, işlenmesi halinde, verilecek ceza yarı oranında artırılır."

137. maddenin (a) bendine göre kişisel verilerin kaydedilmesi suçunun bir kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması suretiyle gerçekleştirilmesi halinde failin cezası yarı oranında artırılarak verilecektir. TCK açısından kamu görevlisinin tanımı ise 6. maddenin (c) bendinde yapılmıştır. Buna göre *"kamu görevlisi deyiminden; kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi"* anlaşılacaktır.

137. maddenin (b) bendine göre ise belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle bu suçun gerçekleştirilmesi hâlinde faile cezası yine yarı oranında artırılarak verilecektir. Burada geçen *"belli bir meslek ve sanat"* kavramından bilişim sektörüyle ve bu sektörün teknik kısmıyla ilgili bir iş kolu anlaşılmalıdır.

Burada değinilmesi ve eleştirilmesi gereken bir konu da, 135. maddenin 2. fıkrasında suçun konusuna ilişkin olarak belirtilen *"nitelikli kişisel verilerin"* düzenlenmesidir. Bu fıkrada *"Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veriolarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır"* denilmektedir. Meclis alt komisyonu tarafından kabul edilen ceza yasası tasarısında bu nitelikli kişisel verilerin suçun konusunu oluşturması cezanın artırılmasına neden olan nitelikli hâl olarak öngörülmüştü. Ancak Adalet Komisyonu tarafından genel kurula gönderilen ve genel kurulda kabul edilerek yasalaşan metinde nitelikli kişisel verilerin suçun konusunu oluşturması hâli cezayı artıran nitelikli hâl olarak öngörülmemiştir. Bu durumda söz konusu verileri ayrıca belirtmenin yasa yapma tekniği açısından bir anlamı kalmamıştır. Oysa alt komisyonda kabul edilen metinde olduğu gibi bu verilerin suçun konusunu oluşturması hâlinin cezayı artıran nitelikli hâl olarak öngörülmesi daha yerinde bir düzenleme olacaktı.

Bu fıkrada yer alan konulardan örneğin sağlık durumu bilgisi, bir kişiye yönelik olarak değil, *"x bölgesinde ... hastalığı yaygındır"* şeklinde genel olarak kaydedilmişse yani istatistikî bir bilgi niteliğinde ise bu fıkraya göre suç oluşmayacaktır. Çünkü bu durumda bilgi, kişisel veri niteliğinde kayıt edilmemiştir.[87]

e. Hukuka Aykırılık Unsuru

TCK'nın 135. ve 136. maddelerdeki suçların tanımında failin eylemlerini *"hukuka aykırı olarak"* gerçekleştirmesi gerektiği ayrıca ifade edilmiştir. Öğretide bizim de katıldığımız şu an için azınlıkta olan görüşte ise, bazen suç tipinde bu ve buna benzer kavramların, genel hukuka uygunluk sebebinin yokluğuna işaret etmek üzere gereksiz kullanıldığı, burada yasa koyucunun, yargıcı, hukuka uygunluk nedenlerinin varlığı konusu üzerinde hassasiyetle durması konusunda uyardığı ancak bu tür hukuka aykırılığın kastın kapsamında olmasının gerekmediği, dolayısıyla bunun suç tanımına ait olmadığı ifade edilmektedir. Nitekim TCK'nın 135. ve 136/1.

87 Dülger, s.567.

maddesindeki suçlarda "hukuka aykırı olarak" ifadesi bu anlamda kullanılmıştır. Dolayısıyla bizim kabul ettiğimiz görüşe göre suç tanımında yer alan bu ifadenin özel bir anlamı olmayıp bunlar suç tipine dahil değildir.

Kişisel verilerin kaydedilmesi suçunda mağdurun rızası ya da yasayla verilen yetki, eylemi hukuka uygun hale getirecektir. Kişinin, verinin sahibi ya da ilgilisi tarafından verilen bir izne dayanarak verileri kaydetmesi durumunda suç oluşmayacaktır.Yasanın verdiği yetkiye dayanılarak kişisel veri kaydedilmesi diğer bir hukuka uygunluk sebebidir.[88]

f. Suçun Özel Görünüş Biçimleri

aa. Teşebbüs: Kişisel verilerin kaydedilmesisuçunun teşebbüs hâlinde kalması mümkündür. Teşebbüs hâli, fail tarafından icra hareketlerine başlandıktan sonra bu hareketlerin yarıda kalması şeklinde olabilecek ya da icra hareketleri tamamlansa bile failin elinde olmayan nedenlerle kaydetme neticesinin gerçekleşmemesi nedeniyle suç teşebbüs aşamasında kalabilecektir.[89]

bb. İştirak: Suça iştirak açısından bir özellik söz konusu olmayıp TCK'nın 37., 38., 39. ve 40. maddelerinde düzenlenen suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir.

Ancak suça iştirak edenlerin kamu görevlisi sıfatını taşıması ya da bu konuyla ilgili belli bir meslek veya sanat sahibi olması hâlinde bu kişilere TCK'nın 137. maddesi gereğince ceza artırılarak verilecektir.[90]

cc. İçtima: Bu suç ile içtima sorunu ortaya çıkması en olası suç, 244. maddenin 1. ve 2. fıkralarında düzenlenen "Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması Suçu ile Verilerin Yok Edilmesi veya Değiştirilmesi Suçu'dur". Özellikle 244. maddenin 2. fıkrasında "sisteme very yerleştiren" ifadesiyle tanımlanan hareketle 135. maddenin eylem unsuru olan "verinin kaydedilmesi" aynı anlama gelmektedir. Ancak iki suç tipi incelendiğinde 135. maddede kişisel verilerin, 244/2'de ise her türlü verinin suçun konusunu oluşturduğu, diğer yandan 244/2'de yalnızca bilişim sistemine veri yerleştirilmesi söz konusu iken 135. maddede bilişim sistemi olsun ya da olmasın kayıt yapmaya elverişli her türlü araca yapılan kayıtın suçun eylem unsurunu oluşturduğu görülmektedir. Buna göre suçun konusu yönünden yalnızca kişisel verileri kapsaması nedeniyle 135. madde, eylem unsuru yönünden yalnızca bilişim sistemlerine yapılan kaydı kapsaması nedeniyle 244. madde diğerine göre "özel norm" niteliğindedir. Bu iki suç tipi arasında öncelikle özel norm – genel norm ayrımına göre bir sonuca ulaşılmaya çalışılmalı, bunun mümkün olmaması hâlinde düşünsel birleşme kuralı uygulanmalıdır.

Bu suçun zincirleme şekilde işlenmesi mümkündür. Bu suçun devam eden suç şeklinde işlenmesi de mümkündür.[91]

88 Dülger, s.568.
89 Dülger, s.588.
90 Dülger, s.588.
91 Dülger, s.588.

g. Yaptırım, Soruşturma ve Kovuşturma

Kişisel verilerin kaydedilmesisuçunu işleyen failler için yalnızca hürriyeti bağlayıcı ceza öngörülmüştür. Yasada bu suçun cezası olarak altı aydan üç yıla kadar hapis cezası düzenlenmiştir.

TCK'nın 140. maddesi gereğince bu suçun işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlaması hâlinde bunlara TCK'nın 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır.[92]

3.3.6.5. Kişisel Verileri Verme veya Ele Geçirme Suçu (m.136)

a. Korunan Hukuksal Değer

TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunda korunan hukuksal değer ile bu suç tipiyle korunan hukuksal değer aynıdır. Kısaca belirtmek gerekirse, bu suç tipiyle genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özel olarak ise kişisel veriler korunmaktadır.[93]

b. Tipikliğin Maddî Unsurları

aa. Fail: Madde metninde suçu işleyecek kişi açısından herhangi bir özellik belirtilmemiştir; bu nedenle bu suçun faili herkes olabilir. Dolayısıyla kişisel verileri verme ve ele geçirme suçu, fail açısından bir özellik göstermemektedir.

Ancak bu suçu işleyenin kamu görevlisi olması TCK'nın 137. maddesi açısından cezayı artırıcı nitelikli hal olarak öngörüldüğü için failin kamu görevlisi olması durumu ceza belirlenirken dikkate alınacaktır.[94]

bb. Mağdur: Kişisel verileri verme veya ele geçirme suçunda herkes suçun mağduru olabilir, suç tipi bu açıdan bir özellik göstermemektedir. Bu suçun mağduru olmak için mutlaka bilişimsistemine kaydedilen verilerin maliki veya zilyedi olunması gerekmemektedir; önemli olan verilen, yayılan ya da ele geçirilen kişisel verilerin bireyle ilgili olmasıdır.[95]

cc. Suçun Konusu: Bu suçun konusunu *"kişisel veriler"* oluşturmaktadır. Kişisel verileri verme ve ele geçirme suçunun konusuyla 135. maddede düzenlenen kişisel verileri kaydetme suçunun konusu tamamen aynıdır; bu nedenle 135. maddede konu açısından yapılan geniş açıklama aynen bu suç tipi açısından da geçerlidir.

Uygulamada Yargıtay, kişisel verilerin yayılması suçuna ilişkin vermiş olduğu bir kararında telefon numaralarının da kişisel veri olduğunu belirtmiştir. Biz de bu görüşe katılıyoruz.[96]

92 Dülger, s.589.
93 Dülger, s.589.
94 Dülger, s.590.
95 Dülger, s.590.
96 Dülger, s.590.

dd. Eylem:

aaa. Kişisel Verilerin Başkasına Verilmesi: Kişisel verilerin başkasına verilmesi çok çeşitli yöntemlerle gerçekleştirilebilecektir. Buna örnek olarak, yazılı verilerin elden ya da posta yoluyla verilmesi veya sanal ortamda bulunan kişisel verilerin bir "cd-rom" üzerine kaydedilerek ya da internet üzerinden elektronik posta şeklinde gönderilmesi yoluyla verilmesi gösterilebilir.

Kişisel verilerin bizzat sır saklama yükümlülüğü olan ancak söz konusu kişisel veriyi öğrenmesinde bir yarar bulunmayan ya da konuyla ilgisiz olan bir başka kişiye, örneğin hastanın tedavisine katılmayan bir hekime verilmesi de suç oluşturacaktır. Ancak sağlık personelinin kendi arasında hastanın tedavisi amacıyla bilgi alışverişi için hastaya ilişkin bazı verileri birbirine aktarması 136. maddede düzenlenen verme ve yayma olarak kabul edilmemelidir.[97]

Kişisel verilerin başkasına verilmesi hareketinde yer alan "başkası" gerçek kişiler olabileceği gibi tüzel kişiler de olabilecektir. Failin kişisel verileri suçun mağduru dışındaki gerçek veya tüzel bir kişiye verileri vermesi hâlinde suç gerçekleşmiş olacaktır.

bbb. Kişisel Verilerin Yayılması: Kişisel verilerin yayılması da çok çeşitli şekillerle gerçekleştirilebilecektir. Bu, kişisel verilerin yazılı olarak mektup şeklinde birden fazla kişiye gönderilmesiyle gerçekleştirilebileceği gibi, internet üzerinde bir web sitesinde kişisel verileri başkaları için erişilebilir kılmak, bir forum odasında açıklama yapmak ya da twitter veya facebook'da yayınlamak suretiyle gerçekleştirilebilecektir. Benzer bir şekilde toplu elektronik posta ya da SMS (kısa mesaj) gönderilmesi halleri de yaymak hareketi içinde değerlendirilmelidir. Kişisel verilerin bir tek kişiye verilmesi veya açıklanması suçun oluşması açısından yeterlidir, herkesin bu bilgileri öğrenmesi gerekmemektedir. Kişisel verilerin yayılması eylemi yazılı, görsel ya da sanal basın yoluyla da yapılabilecektir. Verileri yaymadan kastedilen verilerin içeriğinin birçok kişinin öğrenebileceği şekilde başkalarının bilgisine sunulmasıdır; yaymaya örnek olarak kişisel verilerin bir yayında kimlik belirtilmek suretiyle yayınlanması da gösterilebilir.[98]

ccc. Kişisel Verilerin Ele Geçirilmesi: Bu suç tipinin üçüncü seçimlik hareketi olan kişisel verilerin ele geçirilmesi, kişisel verilerin üzerinde yazılı olduğu belgelerin bulunduğu yerden alınması suretiyle meydana getirilebileceği gibi, verilerin kayıtlı olduğu bilişim sistemine girilerek verilerin bir USB'ye kaydedilmesi ve USB'nin alınması yoluyla da yapılabilecektir. Dolayısıyla kişisel verilerin ele geçirilmesine yönelik tüm yöntemler buna dahil olacaktır.[99]

c. Tipikliğin Manevî Unsuru:

Bu suçun manevî unsuru kasttır. Suç tipinde açıkça belirtilmediği için bu suçun taksirle işlenmesi mümkün değildir.[100]

97 Dülger, s.591.
98 Dülger, s.591.
99 Dülger, s.592.
100 Dülger, s.593.

d. Suçun Nitelikli Hâlleri:

TCK'nın 137. maddesinde "nitelikli hâller" başlığı altında özel hayata ve hayatın gizli alanına karşı suçlar bölümünde yer alan suçlar için failin sıfatından kaynaklanan cezayı artıran nitelikli haller öngörülmüştür. Buna göre söz konusu nitelikli hallerden herhangi birisinin gerçekleşmesi halinde faile verilecek ceza yarı oranında artırılacaktır.[101]

e. Hukuka Aykırılık Unsuru:

Bu suç tipi açısından mağdurun rızasıya da yasayla verilen yetkieylemi hukuka uygun hâle getirecektir. Kişinin, verinin sahibi ya da ilgilisi tarafından verilen bir izne dayanarak kişisel verileri vermesi, yayması veya ele geçirmesi ya da görevli bir kişinin yasadan aldığı yetkiye dayanarak aynı eylemleri gerçekleştirmesi durumunda suç oluşmayacaktır.

Bunun dışında 135. maddenin hukuka aykırılık unsuru konusunda açıklanan nedenler ve suçun özellikle hukuka aykırı olarak işlenmesinin suç tipinde belirtilmesi hususunda yapılan açıklamalar, kişisel verileri hukuka aykırı olarak verme veya ele geçirmesuçu açısından da geçerlidir.

Bu suça ilişkin ilginç bir husus ise kişinin rızasıyla verdiği bilişim sistemine giriş kodlarını içeren şifrelerin işten ayrılan ya da çıkartılan işçi tarafından geri verilmemesi halinde bunun hangi suçu oluşturacağıdır. Öncelikle ifade etmeliyiz ki burada ilgilisinin rızası bulunduğu için 136. madde yer alan kişisel verilerin ele geçirilmesi suçu söz konusu olmamaktadır. Başlangıçtaki rıza bu suçun oluşmasını engellemektedir. Öte yandan failin zilyetliğine bırakılmış malın iadesi istendiğinde inkarı durumunun söz konusu olup olmadığının üzerinde durulmalıdır. Bize göre bu şifrenin iade edilmemesi ile ekonomik değeri olan bir sisteme ya da siteye giriş tamamen imkânsız hale geliyorsa, aynen bilişim sistemiyle hırsızlıkta olduğu gibi bu şifrenin de ekonomik bir değer ifade ettiğinden bahisle, şifrenin iade edilmemesi hâlinde zilyetliğin inklârı olgusunun söz konusu olduğu ve TCK'nın 155. maddesinde yer alan güveni kötüye kullanma suçunun oluşacağı söylenebilecektir. Ancak bu yorumun TCK'nın 2. maddesinde düzenlenen genişletici yorum yasağına takılması kuvvetle muhtemel olacaktır. Öte yandan eski çalışana verilen bu şifre dışında da sisteme erişmek mümkün olduğunda zaten zilyetliğin inkârı durumu söz konusu olmayacak ve suç da gerçekleşmemiş olacaktır. Yargıtay ise önüne gelen somut bir uyuşmazlıkta yukarıda akıl yürütmeye çalıştığımız bu teorik tartışmalara girmeden, şifrenin mal olarak kabul edilmesinin mümkün olmadığından bahisle burada güveni kötüye kullanma suçunun oluşmayacağına karar vermiştir.[102]

f. Suçun Özel Görünüş Biçimleri

aa. Teşebbüs: Kişisel verileri hukuka aykırı olarak verme ve ele geçirme suçunun teşebbüs halinde kalması mümkündür. Suçun maddî unsurunu oluşturan hareketlerin parçalara ayrılabilmesi hâlinde suç teşebbüs aşamasında kalmış olacaktır. Ancak suçun oluşması açısından ayrıca bir neticeye yer verilmediği için, bu suçun teşebbüs aşamasında kalmasına sıklıkla rastlanmayacaktır.[103]

101 Dülger, s.593.

102 Dülger, s.593.

103 Dülger, s.594.

bb. İştirak: Suça iştirak açısından bir özellik söz konusu olmayıp suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir. Ancak suça iştirak edenlerin kamu görevlisi sıfatını taşıması ya da bu konuyla ilgili belli bir meslek veya sanat sahibi olması hâlinde bu kişilere TCK'nın 137. maddesi gereğince ceza artırılarak verilecektir.[104]

cc. İçtima: Kişisel verileri verme ve ele geçirmesuçunun zincirleme şekilde işlenmesi mümkündür. Örneğin, aynı suç işleme kararıyla kişisel verilerin bir kaç kez yayılması ya da başka kişiye verilmesi durumunda olduğu gibi. Bu durumda fail tek bir suç işlemiş olarak kabul edilecek ancak cezası artırılarak verilecektir.

Bu suçun devam eden şekilde işlenmesi de mümkündür. Bu durumda suç devam eden eylemin bittiği zaman gerçekleşmiş kabul edilecek ve zamanaşımı da bu andan itibaren işlemeye başlayacaktır.

İçtima konusunda 243. madde ile 136. maddenin ilişkisi önemlidir. Zîra pek çok kişisel veri bilişim sistemlerine kaydedilmiş durumdayken, bu sistemlere izinsiz girilmesi suretiyle kişisel veriler ele geçirilmektedir. İşte bu durumda 243. maddenin 136. madde açısından geçit suç olabilmesi söz konusu olmaktadır. Ancak bize göre burada bir geçit suçu hali yoktur. Çünkü geçit suçunun olabilmesi için ilk suç işlenmeden ikincisinin işlenmesinin mümkün olmaması ve suçların aynı hukuksal değeri koruması gerekmektedir. Bu durum ise her şartta gerçekleşmemektedir. Zîra kişisel verilerin ele geçirilmesi için bunların mutlaka bilişim sisteminde kayıtlı olması gerekmemektedir, ayrıca her iki suç tipinin koruduğu değerler de farklıdır. Nitekim öğretide de bir bilişim sistemine girerek oradaki kişisel verileri ele geçiren kişi bakımından bunun dışa yansımasının iki değişiklik şeklinde olduğu, bu durumda hem bilişim sistemine girme ve hem de kişisel verilerin ele geçirilmesinin gerçekleştiği, dolayısıyla bu durumda hem TCK'nın 243. maddesinin hem de TCK'nın 136. maddesinin uygulanmasının gerektiği (gerçek birleşme) ifade edilmektedir.

TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçuyla 136. maddede düzenlenen kişisel verileri hukuka aykırı olarak verme ve ele geçirme suçu arasında da suçların içtiması söz konusu olabilecektir. Örneğin fail düşmanlık beslediği bir kişinin özel yaşantısını yaymak için bu kişi hakkındaki verileri öncelikle kaydetmek zorunda kalabilecektir. Bu durumda da geçit suçu söz konusu olmayacaktır, Zîra kişisel veriler kayıt edilmeden de bunların yayılması, verilmesi ya da ele geçirilmesi mümkündür. Örneğin bulut bilişimde yüklü kişisel verilere erişim için şifrelerin ele geçirilmesi hâlinde kayıt edilmeksizin ele geçirme hareketi yapılmış olmaktadır. Aynı şekilde sanal ortamda kayıtlı başkasına ait kişisel verilerin yayılması hâlinde öncesinde kayıt olmaksızın 136. maddede tanımlı suçun işlenmesi mümkündür, dolayısıyla arada zorunluluk ilişkisi bulunmamaktadır.

Kişisel verinin açıklanmasının aynı zamanda hakaret suçunu da oluşturması hâlinde, bir eylem ile birden fazla suçun oluşumuna neden olunduğu için, bu suçla hakaret suçu arasında düşünsel birleşme söz konusu olacaktır. Failin sorumluluğu en ağır cezayı gerektiren suçtan olacaktır. Bu durumda kişisel verilerin açıklanması suçunun cezası daha fazla olduğu için faile bu suçtan dolayı ceza verilecektir.[105]

104 Dülger, s.594.

105 Dülger, s.595.

g. Yaptırım, Soruşturma ve Kovuşturma

Kişisel verileri hukuka aykırı olarak verme ve ele geçirme suçunu işleyen failler için yalnızca hürriyeti bağlayıcı ceza öngörülmüştür. Yasada bu suçun cezası olarak bir yıldan dört yıla kadar hapis cezası düzenlenmiştir.

TCK'nın 140. maddesi gereğince bu suçun işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlaması hâlinde bunlara TCK'nın 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır.[106]

3.3.6.6. Verilerin Yok Edilmemesi Suçu (TCK m.138)

"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir."

a. Korunan Hukuksal Değer

Bu suç tipiyle iki farklı hukuksal değer korunmaktadır. Bunlardan biri *"kamu idaresinin güvenilirliği ve işleyişi"* diğeri ise *"kişisel verilerin güvenliğidir"*. [107]

b. Tipikliğin Maddî Unsurları

aa. Fail: Bu suçun faili *"verileri sistem içinde yok etmekle görevli olan"* kişidir. Bu görevi ise konuyla ilgili özel yasalarda belirtilecektir; ceza yasasında yerinde olarak bu görevlerin hangi yasalar tarafından verileceği belirtilmemiş ve genel bir ifade kullanılmıştır. Her somut olayda bu yasa belirlenecek ve kimlere nasıl bir veri yok etme görevi verildiği araştırılacaktır.

Fail her ne kadar bu görevi kamu adına yapmaktaysa da TCK'nın 6. maddesinde tanımı verilen "kamu görevlisi" sıfatını taşımak zorunda değildir. Zaten inceleme konusu suç tipi *"özel türde, kendine özgü bir görevi ihmal suçu"* olduğu için failin kamu görevlisi olması aranmamıştır. Dolayısıyla kişisel verilerle ilgili olarak düzenleme yapan bir yasada kamu görevlisi olmayan kişiler için de bu tür görevlerin verilmesi halinde bunlar da inceleme konusu suçun faili olabileceklerdir.[108]

bb. Mağdur: Bu suçun mağduru belli bir birey değildir. Her ne kadar yok edilmeyen kişisel veriler bazı bireylere ait olsalar da yukarıda suçla korunan hukuksal değer konusunda belirtildiği üzere bu suç tipiyle kamu idaresine duyulan güven korunduğu için suçun mağduru da kamu olmaktadır.

Ancak hakkındaki kişisel veri yok edilmeyen kişi suçtan zarar gören kişi olacak ve suçla ilgili olarak yapılan yargılamada katılan sıfatıyla bulunabilecektir.[109]

cc. Suçun Konusu: Bu suçun konusunu "kişisel veriler" oluşturmaktadır. 138. maddede düzenlenen kişisel verileri yok etmeme suçunun konusuyla 135. maddede düzenlenen kişisel verileri kaydetme suçunun ve 136. maddede düzenlenen kişisel

106 Dülger, s.596.
107 Dülger, s.597.
108 Dülger, s.598.
109 Dülger, s.598.

verileri hukuka aykırı olarak verme ve ele geçirme suçunun konusu tamamen aynıdır; bu nedenle 135. maddede suçun konusu açısından yapılan açıklama bu suç tipi açısından da aynen geçerlidir.[110]

dd. Eylem: Bu suçun hareket unsuru birbirine bağlı iki farklı hareketten oluşmaktadır. Öncelikle failin kişisel verileri yok etmek hususunda, herhangi bir hukuksal düzenlemeden kaynaklanan yükümlülüğü bulunmalı ve bu düzenlemede yer alan verinin saklanması süresini geçirmiş olmalıdır. Buna bağlı olarak da bu sürenin geçmesi akabinde suçun konusunu oluşturan veriyi yok etmemesi ile suç gerçekleşmiş olmaktadır.

Verileri yok etmeme suçu açısından ayrıca bir netice aranmamaktadır. Söz konusu ihmali hareketin yapılmasıyla suç gerçekleşmiş olmaktadır. Dolayısıyla bu suç, zarar suç olmadığı gibi soyut tehlike suçudur.[111]

c. Tipikliğin Manevî Unsuru

Bu suçun manevî unsuru kasttır, suçun taksirle işlenmesi mümkün değildir.[112]

d. Hukuka Aykırılık Unsuru

Yasa'nın 138. maddesinde düzenlenen kişisel verilerin yok edilmemesi suçunda iki farklı hukuksal değerin korunduğu ve buna bağlı olarak hem kişisel verilerin ilgilisi olan birey, hem de toplumu oluşturan her birey suçun mağduru olduğu için; yok edilmeyen verilerin ilgilisi olmasına rağmen suçtan zarar gören kişinin rızası eylemi hukuka uygun hale getirmeyecektir.[113]

e. Suçun Özel Görünüş Biçimleri

aa. Teşebbüs: Bu suç tipi maddî unsur konusunda belirtildiği üzere ihmal suretiyle işlenebilmektedir. Dolayısıyla bu suçun gerçekleştirilmesine yönelik eylemlerin teşebbüs derecesinde kalması mümkün değildir.[114]

bb. İştirak: Bu suça iştirakin gerçekleşmesi mümkündür. Suça iştirak açısından bir özellik söz konusu olmayıp suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir. Ancak bu suç tipi açısından 39. maddenin 2. fıkrasının "b" ve "c" bentlerinde yer alan suça iştirak çeşitlerinin gerçekleşmesi pek mümkün görülmemektedir.[115]

cc. İçtima: Verileri yok etmeme suçunun zincirleme şekilde işlenmesi mümkündür. Örneğin aynı suç işleme kastıyla kişisel verilerin ardı ardına yok edilmemesi durumunda olduğu gibi. Bu durumda fail tek bir suç işlemiş olarak kabul edilecek ancak cezası arttırılarak verilecektir.[116]

Ayrıca 138. madde yer alan kişisel verilerin yok edilmemesi suçu tanımı gereği

110 Dülger, s.598.
111 Dülger, s.599.
112 Dülger, s.601.
113 Dülger, s.601.
114 Dülger, s.602.
115 Dülger, s.602.
116 Dülger, s.602.

devam eden suç (mütemadi) niteliğindedir. Fail hakkında idari veya cezai soruşturma başlatılana ya da bu durum tespit edilene kadar suç devam edecektir.[117]

f. Yaptırım, Soruşturma ve Kovuşturma

Kişisel verileri yok etmeme suçunu işleyen failler için yalnızca hürriyeti bağlayıcı ceza öngörülmüştür. Yasada bu suçun cezası olarak altı aydan bir yıla kadar hapis cezası düzenlenmiştir.

TCK'nın 140. maddesi gereğince bu suçun işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlaması halinde bunlara TCK'nın 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır.[118]

3.3.7. Devlet Sırlarına Karşı Suçlar (TCK 326/1, 327,329, 330, 333, 334, 335, 336, 337)

3.3.7.1. Devletin Güvenliğine İlişkin Belgeler

"Madde 326

(1) Devletin güvenliğine veya iç veya dış siyasal yararlarına ilişkin belge veya vesikaları kısmen veya tamamen yok eden, tahrip eden veya bunlar üzerinde sahtecilik yapan veya geçici de olsa, bunları tahsis olundukları yerden başka bir yerde kullanan, hileyle alan veya çalan kimseye sekiz yıldan oniki yıla kadar hapis cezası verilir.

(2) Yukarıdaki yazılı fiiller, savaş sırasında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye koymuş ise müebbet hapis cezası verilir."

Madde metni 765 sayılı TCK'nın 132. maddesinin 1. fıkrasından alınmış, suç unsurları muhafaza edilmiş, cezanın üst sınırı azaltılmıştır. Korunan hukukî yarar ülke güvenliğidir. Suçun maddî unsuru belge veya vesikaları kısmen veya tamamen yok etmek, ortadan kaldırmak, tahrip etmek, üzerlerinde sahtecilik yapmak, bulundukları yerden başka bir yerde kullanmak, hile ile almak veya çalmaktır. Maddenin uygulanması için kâğıt veya belgelerin bir sırrı ihtiva etmesi zaruri değildir. Korunan, belgenin ihtiva eylediği sır değil, devletin güvenliğine veya siyasal menfaatlerine ilişkin belge ya da evraktır. Bu belge ya da evrak elektronik ortamda saklanması durumunda bilişim yolu ile bu belgelere ulaşma ve bunları tahrip etme mümkün olabilecektir.

Bkz. Askeri Yargıtay Daireler Kurulunun 21/06/2007 tarih ve 2007/83 Esas, 2007/81 Karar sayılı kararı.

3.3.7.2. Devletin Güvenliğine İlişkin Bilgileri Temin Etme

"Madde 327

(1) Devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgileri temin eden kimseye üç yıldan sekiz yıla kadar hapis cezası verilir.

(2) Fiil, savaş sırasında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye koymuşsa müebbet hapis cezası verilir."

117 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s.602.

118 Dülger, s.602.

Madde metni 765 sayılı TCK'nun 132. maddesinin son fıkrasındaki hükümlere karşılık olarak düzenlenmiş olup suç unsurları aynen muhafaza edilmiştir. Korunan hukukî yarar, milli savunmadır. Suçun maddî unsuru gizli kalması gereken bilgileri temin etmektir. Madde metninde "temin etme" şeklinde tek bir hareket ön görülmüş ise de bu değişik yollarla olabilir. Temin etmenin bilişim yolu ile olması da mümkündür.

Askerî Yargıtay Daireler Kurulunun 21/06/2007 tarih ve 2007/83 Esas, 2007/81 Karar sayılı kararı.

3.3.7.3. Devletin Güvenliğine ve Siyasal Yararlarına İlişkin Bilgileri Açıklama

"Madde 329

(1) Devletin güvenliği veya iç veya dış siyasal yararları bakımından niteliği itibarıyla gizli kalması gereken bilgileri açıklayan kimseye beş yıldan on yıla kadar hapis cezası verilir.

(2) Fiil, savaş zamanında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye koymuşsa, faile on yıldan onbeş yıla kadar hapis cezası verilir.

(3) Fiil, failin taksiri sonucu meydana gelmiş ise birinci fıkrada yazılı olan hâlde, faile altı aydan iki yıla, ikinci fıkrada yazılı hâllerden birinin varlığı hâlinde ise üç yıldan sekiz yıla kadar hapis cezası verilir."

Madde metni 765 sayılı TCK'nın 136. maddesinin 1, 2 ve 5. fıkralarında düzenlenen devlet sırlarını ifşa başlığı altındaki hükümlerdir. Korunan hukukî yarar milli savunmadır. Suçun maddî unsuru niteliği itibari ile gizli kalması gereken bilgileri açıklamak (ifşa etmektir). Gizli bilgilerin devletin güvenliğine, iç veya dış siyasal yararlarına ait olup, niteliği itibari ile gizli kalmasının gerekmesi yani sır olması lazımdır. Bir veya birkaç kişiye açıklamanın yapılması yeterlidir. Umuma yapılması gerekmez. Son fıkradaki fiile taksirle sebebiyet verme hâlinde ise, yapılan açıklama değil, sırrın failin taksiri sonucu açıklayanın eline geçmesi hali kastedilmektedir. 329. maddesinin 1. ve 2. fıkralarındaki suçun bilişim yoluyla işlenmesi pekâlâ mümkün olduğu gibi, devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri muhafaza etmekle görevli (örneğin bilgisayar kütüklerinde saklanan bir veri) kişi ya da kişilerin kusurları sonucunda bu bilgilerin başkaları tarafından bilişim yoluyla ele geçirilmesi durumu da mümkündür.
Bkz. Askerî Yargıtay Daireler Kurulunun 21/06/2007 tarih ve 2007/83 Esas, 2007/81 Karar sayılı kararı.

3.3.7.4. Gizli Kalması Gereken Bilgileri Açıklama

"Madde 330

(1) Devletin güvenliği veya iç veya dış siyasal yararları bakımından niteliği itibarıyla gizli kalması gereken bilgileri siyasal veya askerî casusluk maksadıyla açıklayan kimseye müebbet hapis cezası verilir.

(2) Fiil, savaş zamanında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeyle karşı karşıya bırakmış ise, faile ağırlaştırılmış müebbet hapis cezası verilir."

Madde metni 765 sayılı TCK'nın 136. maddesinin 1. fıkrasındaki suç tipinin ağırlaştırıcı sebebi olarak ön görülen hükmün (siyasi veya askeri casusluk maksadıyla hareket etme) ayrı bir suç haline getirilmesi ile oluşturulmuştur. Suçun maddî unsuru

gizli kalması gereken bilgileri casusluk maksadı ile açıklamaktır. Bilgiler gizli mahiyette olmalı ve devletin güvenliği, iç veya dış siyasal yararlarına ilişkin bulunmalıdır. Siyasi casusluk, yabancı bir devlet yararına Türkiye Devletinin veya vatandaşlarının veya oturanların zararına bilgilerin toplanması, askeri casusluk ise yabancı devlet yararına ve Türkiye Cumhuriyeti zararına askerî bilgilerin toplanmasıdır.

3.3.7.5. Devlet Sırlarından Yararlanma, Devlet Hizmetlerinde Sadakatsizlik

"Madde 333

(1) Görevi dolayısıyla öğrendiği ve Devletin güvenliğinin gizli kalmasını gerektirdiği fenni keşif veya yeni buluşları veya sınaî yenilikleri kendisinin veya başkasının yararına kullanan veya kullanılmasını sağlayan kişi, beş yıldan on yıla kadar hapis ve üçbin güne kadar adlî para cezası ile cezalandırılır.

(2) Fiil, Türkiye ile savaş hâlinde bulunan bir devletin yararına işlenir veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye sokacak olursa, faile müebbet hapis cezası verilir.

(3) Türkiye Devleti tarafından yabancı bir memlekette Devlete ait belirli bir işi görmek için görevlendirilen kimse, bu görevi sadakatle yerine getirmediği ve bu fiilden dolayı zarar meydana gelebildiği takdirde faile beş yıldan on yıla kadar hapis cezası verilir.

(4) Bu maddede tanımlanan suçların işleneceğini haber alıp da bunları zamanında yetkililere ihbar etmeyenlere, suç teşebbüs derecesinde kalmış olsa bile altı aydan iki yıla kadar hapis cezası verilir."

Madde metni 765 sayılı TCK'nın 138. maddesinde düzenlenen hükmün kısmen tekrarıdır. Eski Yasadaki suçun müttefikler zararına işlenmesi hâline yer verilmemiştir. Korunan hukukî yarar 1. fıkrada devletin güvenliği açısından gizli kalması gereken fenni ve sınai sırların açıklanmasının önlenmesi, 3. fıkradaki göreve sadakatsizlik suçunda ise devlet adına görevli kişinin sadakatla görevini yerine getirmesinin temini, son fıkradaki suçta ise bu tür suçların önüne geçilmesi suretiyle devlet güvenliğinin sağlanmasıdır.

3.3.7.6. Yasaklanan Bilgileri Temin

"Madde 334

(1) Yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri temin eden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Fiil, Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeyle karşı karşıya bırakmış ise faile beş yıldan on yıla kadar hapis cezası verilir."

3.3.7.7. Yasaklanan Bilgilerin Casusluk Maksadıyla Temini

"Madde 335

(1) Yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri siyasal veya askerî casusluk maksadıyla temin eden kimseye sekiz yıldan oniki yıla kadar hapis cezası verilir.

(2) Fiil, Türkiye ile savaş hâlinde bulunan bir devletin yararına işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeyle

karşı karşıya bırakmış ise faile ağırlaştırılmış müebbet hapis cezası verilir."

Yasaklanan bilgilerin temini 5237 s.Y. 334. maddesinde, yasaklanan bilgilerin casusluk maksadıyla temini ise 5237 s.Y. 335. maddede düzenlenmiştir. 334. madde metini 765 sayılı TCK'nun 132. maddesinin 3. ve 4. fıkralarının karşılığı olarak düzenlemiş, 335. madde metni ise, 765 sayıl TCK'nun 133. maddesinin 2., 3. ve 4. fıkralarında yer alan hükümlerin suçun unsurlarının korunarak yeniden düzenlenmesinden ibarettir.

334. maddede korunan hukukî yarar millî savunma ve kamu güvenliğidir. Gizli kalması gereken ve açıklanması yasaklanan bilgileri temin etmek suçun maddî unsur olup suç bilginin temin edilmesi ile (öğrenilmesiyle) tamamlanmış olur. Bilgilerin bulunduğu belgelerinde elde edilmesi veya temin edilen bilgilerin başkasına verilmesi suçun tamamlanması için şart değildir. Suçun oluşması için Kanun ve düzenleyici işlemlerin yetkili makamlara o konudaki bilgilerin açıklanmasını yasaklama yetkisini vermiş bulunması ve bu şekilde söz konusu bilgilerin niteliği bakımından gizli kalması zorunlu olmalıdır.

335. maddede korunan yarar ülke güvenliğidir. Açıklanması yasaklanan ve niteliği gereği gizli kalması gereken bilgileri, siyasi ve askerî casusluk maksadıyla temin etmek etmek suçun maddî unsuru olup bilgileri elde etmede kullanılan vasıtanın veya bilgilerin yer aldığı belgelerinde elde edilmiş olup olmamasının suça bir etkisi yoktur. Bilgilerin mevzuat gereği yasaklanmış olması ve niteliği itibari ile gizli kalmasının gerekmesi şart olmalıdır. Failde casusluk kastı belirlenemez ise 334. maddedeki suç düşünülmelidir.

Aynı şekilde bu suçunda bilişim sistemleri kullanılmak suretiyle işlenmesi söz konusu olabilir. Maddede tarif olunan ve gizli kalması gereken bilgiler elektronik ortamda, bilgisayar kütüğünde vb. dijital depolama aygıtlarında tutulması ve bu bilgilerin buralardan temin edilmesi hâli mümkündür.

3.3.7.8. Yasaklanan Bilgileri Açıklama

"Madde 336

(1) Yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri açıklayan kimseye üç yıldan beş yıla kadar hapis cezası verilir.

(2) Fiil, savaş zamanında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye sokmuş ise faile on yıldan onbeş yıla kadar hapis cezası verilir.

(3) Fiil, failin taksiri sonucu meydana gelmiş ise, birinci fıkrada yazılı olan hâlde faile altı aydan iki yıla, ikinci fıkrada yazılı hâlde üç yıldan sekiz yıla kadar hapis cezası verilir."

3.3.7.9. Yasaklanan Bilgileri Siyasal veya Askerî Casusluk Maksadıyla Açıklama

"Madde 337

(1) Yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri, siyasal veya askerî casusluk maksadıyla açıklayan kimseye on yıldan onbeş yıla kadar hapis cezası verilir.

(2) Fiil, savaş zamanında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeyle karşı karşıya bırakmış ise ağırlaştırılmış müebbet hapis cezası verilir."

Yasaklanan bilgileri açıklama 5237 s.Y. 336. maddesinde, yasaklanan bilgilerin siyasal veya askerî casusluk maksadıyla açıklama ise 5237 s.Y. 337. maddesinde düzenlenmiştir. 336. madde metini 765 sayılı TCK'nın 137. maddesinin 1., 2. ve son fıkralarında yer alan hükümlerin karşılığı olarak düzenlemiş olup 337. madde metni ise 765 sayılı TCK'nın 137. maddesinin 3. fıkrasında yer alan hükmün ve 2. fıkrasında yer alan ağırlaştırıcı sebebin tekrarıdır.

336. ve 337. maddelerde korunan hukukî yarar millî savunma ve devletin güvenliğidir. 336. maddede suçun maddî unsuru açıklanması yasaklanan ve niteliği itibariyle gizli kalması gereken bilgileri açıklamaktır. 337. maddede ise bu açıklamanın askerî ve siyasi casusluk maksadıyla yapılması düzenlenmiştir. Yasaklama kanun, tüzük ve yönetmeliklere göre yapılmalı, bilgi ise niteliği itibariyle gizli kalması gerekli bilgilerden olmalıdır. 1. ve 2. fıkralardaki suç kastla işlenebilir, 3. fıkradaki suç taksirle işlenebilir.

Asker kişinin evinde yapılan aramada ele geçirilen özel kuvvetlere ilişkin CD içeriğinde devletin güvenliği veya iç veya dış siyasal yararları bakımında gizli kalması gereken nitelikte bilgiler olup olmadığına dair bkz. Askeri Yargıtay Daireler Kurulunun 21/06/2007 tarih ve 2007/83 Esas, 2007/81 Karar sayılı kararı.

Yukarıda sayılan maddelerde geçen suçların pek tabi bilişim sistemleri aracı kılınmak suretiyle işlenmesi mümkündür. Örneğin devletin güvenliğine ve siyasal yararlarına ilişkin bilgiler kendisinde bulunan kişi bunları dijital ortamda saklayabileceği gibi, dijital ortamlarda kullanılan veri saklama aygıtlarında da (flash bellek, CD, DVD, harddisk, disket, hafıza kartları vb.) tutabilir. Bu bilgileri kullandığı bilgisayarında saklayan bir kişinin bunları kendi arzu ve isteği ile başkalarına iletmesi ya da kusuru ile bilgisayarına başka kişiler tarafından ulaşılması ve saklanılan bilgilere erişilmesi durumunda yukarıda belirtilen birçok suçun bilişim yoluyla işlenmesi mümkündür.

TCK md. 326, 327, 329, 330, 333, 334, 335, 336 ve 337'da düzenlenen suç tipleri ile ilgili olarak CAS Grubu Ortak Raporunda geçen delil etme yöntemleri kullanılabilir.

3.3.8. Fikir ve Sanat Eserleri Kanunu Madde 71

3.3.8.1. Fikir Ve Sanat Eserleri Kanunu'ndaki Mali, Manevî ve Bağlantılı Haklara Tecavüz Suçları (FSEK M.71)

a. Korunan Hukuksal Değer

İnceleme konusu suç tiplerinden 71. maddede bilişim yazılımlarıyla ilgili hak sahibinin maddî ve manevî hakları ile bağlantılı haklara tecavüz eylemleri düzenlenmiştir. Bunlardan mali haklara yönelik eylemler ile bilişim yazılımları üzerinde tasarruf yetkisi bulunan mağdurun malvarlığında bir azalmaya neden olunacağı görülmektedir. Failin gerçekleştirdiği, yazılımları hukuka aykırı olarak çoğaltmak ya da kullanmak eylemleri sonucunda, yazılım üzerinde hak sahibi olan kişinin bu yazılımla elde ettiği ya da elde etmeyi beklediği gelirde kaçınılmaz olarak bir azalma olacaktır.

Bu nedenle 71. maddede düzenlenen bu eylemlerin malvarlığı aleyhine işlenen suçlar olduğunu ve korunan hukuksal değerin kişinin malvarlığı olduğunu düşünmekteyiz.

FSEK'in 71. maddesinde düzenlenen bilgisayar programları ile ilgili hak sahibinin manevî haklarına yönelik eylemler açısından ise farklı bir durum görülmektedir. Manevî haklar eser sahibi olmanın bir sonucudur. Bu hak, eser sahibinin eseri yaratmış olmasının sonucu olarak kişiye sıkı sıkıya bağlı, başkasına devredilemeyen, vazgeçilemeyen, miras yolu ile mirasçılara geçmeyen ve ne sağlar arası ne de ölüme bağlı tasarrufa konu olmayan haklardandır. Aslında, eser sahibinin manevî ve mali hakları bir bütün oluşturmaktadır ve eser sahipliğinin hukukî sonucudur. Manevî ve maddî hakların ikiye ayrılarak iki hak türü oluşturması aslında teorik bir ayrımdır; bu ayrım günümüz ekonomik ilişkilerinde, eser sahibinin yarattığı eserden ticari olarak faydalanabilmeyi sağlamak amacıyla gerçekleştirilen bir ayrımdır. Ancak FSEK'de bu şekilde bir düzenleme söz konusu olduğu için öğretide ve uygulama konuyu bu şekilde değerlendirmektedir. Madde başlığında da görüldüğü üzere bu suçla ayrıca yazılımüzerinde hak sahibi olan kişinin manevi haklarına yönelik hukuka aykırı eylemler cezalandırılmaktadır. Bir yazılım sahibinin manevî hakları olarak yazılımı kamuya sunma hakkı(FSEK m.14), yazılım sahibinin adını belirtme hakkı yani eser sahibi olarak tanıtılma hakkı (FSEK m.15/1), yazılımda değişiklik yapılmasını yasaklama hakkı(FSEK m.16 ve m.17/1) ve yazılım sahibinin zilyet ve malike karşı hakları yani eser sahibinin eserin aslına varma hakları (FSEK m.17/2) bulunmaktadır. İşte bu haklardan birinin ihlali hâlinde fail FSEK m.71 uyarınca cezalandırılacaktır. Buna göre bu suç tipiyle korunan hukuksal değer yazılım sahibinin FSEK'in ilgili maddelerinde belirtilen manevi haklarıdır. Dolayısıyla bu eylemleri, kendine özgü kişilere karşı işlenen suç olarak değerlendirmekteyiz.[119]

b. Tipikliğin Maddî Unsurları

aa. Fail: Manevî haklara tecavüzsuçu açısından; Yasanın 71/1-1. maddesindeki *"henüz alenileşmemiş bir eseri hak sahibi kişilerin yazılı izni olmaksızın her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten veya yayımlayan"*, 71/1-4. maddesindeki *"henüz alenileşmemiş bir eserin içeriğini ifşa eden"*, 71/1-1. maddesindeki *"bir eseri yazılı izin olmaksızın değiştiren"*, 71/2. maddesinde *"başkasının eserini sahiplenen"*, 71/1-3 ve 71/1-5. maddelerindeki *"intihal eylemlerini gerçekleştiren"* kişiler bu suçun faili olacaklardır.

Maddî haklara tecavüz açısından ise fail; hak sahibi kişilerin yazılı izni olmaksızın eseri işleyen, çoğaltan, yayan, temsil eden, kamuya elektronik aletlerle ileten, ticari amaçla satın alan, ithal eden veya ihraç eden ve kişisel ihtiyacı dışında elinde bulunduran veya depolayan kişidir.[120]

bb. Mağdur: İnceleme konusu suçlar açısından mağdurun tespiti önem taşımaktadır; çünkü her üç suç da FSEK'in 75. maddesi gereğince takibi şikâyete bağlı suçlardır. Bu nedenle ancak hakları tecavüze uğrayan mağdurun şikâyeti hâlinde soruşturma yapılacak ve eylemin sabit görülmesi hâlinde fail cezalandırılacaktır. FSEK'in 75. maddesinde *"Yapılan şikâyetin geçerli kabul edilebilmesi için hak sahiplerinin veya üyesi oldukları meslek birliklerinin haklarını kanıtlayan"* denilmek suretiyle bu suçların mağdurunun hakları tecavüze uğrayan kimse olduğu belirtilmektedir ancak; FSEK'in ilgili maddeleri gereğince esas hak sahibi eseri (bilişim yazılımını) geliştiren,

119 Dülger, s.619.

120 Dülger, s.619.

üreten, ortaya çıkaran eserin (yazılımın) sahibi olmasına rağmen özellikle eser(yazılım) üzerindeki mali hakların devri söz konusu olabildiğinden bunların her suç tipi açısından belirtilmesi gerekmektedir.

Fikri Mülkiyet Hukuku'nda sahibinin özelliklerini taşıması koşulunun doğal sonucu olarak bir eserin sahibi, onu meydana getiren kişi olarak kabul edilmektedir. Bunun evrensel bir kural olduğu ve kaynağını doğal hukuk öğretisinde bulduğu ifade edilmektedir. Bu nedenle yayımcıların, yapımcıların ve tüzel kişilerin eser sahibi olması mümkün değildir ancak ticari yaşamın getirdiği dayatmalar sonucu bu ilkeden sapılarak istisnalar getirilmiş ve mali haklar açısından eser sahipliğinin devri olanaklı hale getirilmiştir, ancak aynı durum kişiye sıkıca bağlı olan eser üzerindeki manevî haklar açısından geçerli değildir.

FSEK'in 71. maddesinde düzenlenen mali haklara tecavüz suçları açısından mağdurun tespit edilebilmesi için yukarıda yapılan kısa açıklama ışığında yazılım üzerindeki hakkın kime ait olduğunun tespiti gerekir. Bu hak, yazılımı üreten ya da geliştiren kişi ya da kişilere ait olabileceği gibi FSEK'in 8. maddesi gereğince sadece mali haklar açısından yazılımın üretilmesini isteyen tüzel kişiliğin ilgili organına ait de olabilecektir. Ayrıca bu hakların bir ruhsat (lisans) ya da bir sözleşmeyle yapımcıya da yayıncıya devri de mümkündür. Ancak devir alanın tüzel kişi olması hâlinde, hakkın ihlali durumunda artık bunlar suçun mağduru değil, suçtan zarar gören olacaklardır.

FSEK'in 27. maddesi gereğince eser sahibine ait olan mali haklar ölümünden itibaren yetmiş yıl boyunca korunmaya devam ettiği için eser sahibinin mirasçıları da hak sahibi olabileceklerdir. İşte bu nedenle mali haklara yönelik suçların işlenmesi durumunda her somut olayda mağdurun tespit edilmesi gerekecektir, suçun işlendiği anda yazılımüzerindeki haklar kime ait ise mağdur da o kişi olacaktır.

Manevîi hakların ihlal edilmesi durumunda mağdurun belirlenmesi açısından maddî haklara yönelik eylemlerde olduğu gibi bir zorluk çekilmeyecektir. FSEK'in düzenlemesine göre yazılım sahibinin manevî haklarını devretmesi mümkün olmadığı için kendisi hayatta iken manevî haklara yönelik bir suçun işlenmesi durumunda suçun mağduru yazılımın sahibi olacaktır. Kendisi öldükten sonra ise; FSEK'in 19. maddesi gereğince aynı yasanın 14. maddesi ve 15. maddesinin 1. fıkrasında düzenlenen manevi haklara ilişkin yetkilerin 19. maddede sayılan mirasçılara geçeceği belirtilmiştir. Bu kişiler söz konusu manevî haklara mirasçı olmamakta; kendileri yasadan kaynaklanan yeni bir hakka sahip olmaktadırlar. Bu hakların tecavüze uğraması hâli ise 71. maddede suçu oluşturan eylemler arasında sayılarak cezalandırılmıştır. Bu nedenle eser sahibi öldükten sonra yetmiş yıllık koruma süresi içinde FSEK'in 14. maddesi ve 15. maddesinin 1. fıkrasında düzenlenen manevî haklara yönelik bir tecavüz hâlinde yasal hak sahibi olan bu kişiler suçun mağduru olacaklardır.[121]

cc. Suçun Konusu: İnceleme konusu suç tipi açısından suçun konusunu genel olarak her türlü eser, çalışmanın konusuyla ilgili olarak da bilişim yazılımları oluşturmaktadır. 1995 yılında 4110 sayılı Yasa ile FSEK'e özellikle Türkiye'nin imzalamış olduğu uluslararası sözleşmelerden kaynaklanan yükümlülüklerinin yerine getirilmesi ve gelişen teknolojinin sebebiyet verdiği gelişmelere ayak uydurmak amacı ile *"her biçim altında ifade alınan bilgisayarprogramları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları ... eser"* sayılır ifadesi eklenmiştir.

121 Dülger, s.620.

FSEK'in 1/B-g maddesinde ise bilgisayar programları *"bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesi ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmaları"* olarak tanımlanmıştır.

Yazılımlara ilişkin geniş açıklamalar önceki bölümlerde yapıldığı için burada tekrar edilmeyecektir. Ancak bu suçun konusunu oluşturan yazılımları, özellikle 5237 sayılı TCK'nın 244. maddesinde düzenlenen suçun konusunu oluşturan verilerin bütünü olan yazılımlardan ayıran önemli fark bunların eser niteliğinde yazılımlar olmalarıdır. Bunun yanı sıra öğretide internetin en yaygın araçlarından olan ve kendine özgü bir tasarımı ve estetiği bulunan web sitelerinin de FSEK kapsamında bir eser sayılıp sayılmayacağı ve çok sık görülen bu sitelerin aynen başka ad altında aktarımı ya da web sitelerinin sanal alanda çalınması eylemlerinin FSEK'de düzenlenen suç tiplerinin kapsamına girip girmediği dolayısıyla web sitelerinin bu suçun konusu oluşturup oluşturmadığı yönünde tartışmalar sürmektedir.

Bir ürünün FSEK'in düzenleme kapsamında esersayılabilmesi için sahibinin özelliklerini taşıması ve yasada belirtilen eser sınıflarından birine dâhil olması gerekir. Bilişim yazılımlarının ilim ve edebiyat eserleri içinde olduğu FSEK'in 2. maddesinin 1. fıkrasında açıkça belirtilmiştir; yazılımın sahibinin özelliklerini taşıyıp taşımadığı konusu ise her somut olayda değerlendirilecektir. Dolayısıyla kendisini üreten kişinin özelliklerini taşıyan yazılımlar suçun konusunu oluşturacaklardır.

Ayrıca FSEK'de bağımsız olarak yaratılmış eserlerin yanında, önceden yapılmış bir esere sadık kalınarak, onun başka bir şekle dönüştürülmüş hâli olan *"işleme eserler"* de düzenlenmiştir. Özellikle yazılım sektöründe bunlara çok sık rastlanılmaktadır, bugün için kullanım alanı yaygın olan pek çok yazılım önceki yazılımların benzeri ya da geliştirilmiş hâlidir. FSEK'de işleme eserin düzenlendiği 6. maddenin 10. ve 11. bentlerinde bilişim yazılımlarının da işleme eser olabilecekleri belirtilmiştir. İşte bu özelliklere sahip yazılımlar da FSEK'in 71. maddesinde düzenlenen suçun konusunu oluşturmaktadır.

Burada belirtilmesi gereken önemli bir konu da bilişim yazılımlarının tamamının FSEK ile korunmadığı bu nedenle yazılımların belli bölümlerinin suça konu oluşturduğudur. Bir yazılımın mantıksal işlem sırasını ortaya koyan *"yazılım akışı"* ile *"yazılımın kaynak kodu"* incelenen suçların konusunu oluştururken, tüm yazılımları oluşturan mantık aşamaları olan *"algoritma"* ve *"kullanıcı ara yüzeyi"* (ara yüzeyin görsel ve işitsel kısmının orijinal olması durumu hariç) incelenen suçların konusunu oluşturmamaktadır.[122]

dd. Eylem:

aaa. Manevî Haklara Yönelik Suçu Oluşturan Hareketler:

aaaa. Umuma İletmek ve Yayımlamak: 71/1-1'de bir eseri (yazılımı) hak sahibi kişilerin yazılı izni olmaksızın her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma iletmek veya yayımlamak suç olarak düzenlenmektedir (hak sahibinin eseri kamuya sunma hakkına tecavüz). Yasada bu suç *"bir eseri, hak sahibi kişilerin yazılı izni olmaksızın ... her türlü işaret, ses veya*

122 Dülger, s.622.

görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ... kişi hakkında bir yıldan beş yıla kadar hapis veya Adlî para cezasına hükmolunur" şeklinde tanımlanmıştır. Bu eylemle FSEK'in 14. maddesinde düzenlenen esersahibinin eserini (yazılımını) topluma sunması hakkı ihlal edilmektedir. Bilişimyazılımının topluma sunulup sunulmamasını, yayımlama zamanını ve şeklini münhasıran eser (yazılımsahibi belirler. Yazılımın topluma sunulması ekonomik açıdan değerlendirme için de bir ön şart olduğu için önem arz etmektedir. Buna göre bir yazılımın; yazılım sahibinin yazılı izni olmaksızın, aslından çoğaltılarak ticari amaçlarla satılması, dağıtılması veya diğer yöntemlerle ticarete konu edilmesi bu suçu oluşturacaktır. Yazılımın, sahibinin rızasıyla topluma arz edilmiş ya da edilmemiş olması eylemin oluşması açısından önemli değildir.[123]

bbbb. Alenileşmemiş Eserin İçeriği Hakkında Bilgi Vermek: FSEK'in 14. maddesinde yer alan esersahibinin eserini "kamuya sunma hakkının" yani "aleniyet kazandırma hakkının" doğal sonucu olan ve FSEK'in 14/2. maddesinde düzenlenen kamuya sunulmamış bir eserin içeriği hakkında bilgi vermek hakkının ihlaline yönelik olarak FSEK'in 71/1-4. maddesinde hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin içeriği hakkında kamuya bilgi verilmesi suç olarak düzenlenmiştir (eser içeriğinin ifşası).[124]

cccc. Esere Ad Koymak: Yazılımın sahibinin izni olmaksızın, bir esere (yazılıma) ad koymak, bu suçu meydana getiren eylemlerden bir diğeridir. Bu eylemle FSEK'in 15. maddesinde düzenlenen yazılıma ad koyma yetkisi ihlal edilmektedir. Bir yazılıma ad koyma yetkisi yalnızca yazılımın sahibine aittir, bu yetki ancak yazılı bir sözleşmeyle devredilebilir. İzin olmaksızın bir yazılıma ad koyma eylemi manevî haklara yönelik suçu meydana getirecektir. Bir eserin birden fazla kişiye ait olması hâlinde failin esersahiplerinden birisinin adının yerine kendi adını koyması ya da gerçek eser sahiplerinin yanında ayrıca kendi adını yazması hâlinde de suç gerçekleşecektir. Çünkü bu hareketin yapılması suretiyle suçun işlenmesi için failin başkasına ait esere kendi adını koyması yeterlidir, eserde gerçek sahiplerinin isimlerinin bulunması ya da bulunmasının suçun oluşumuna etkisi yoktur.[125]

dddd. Tanınmış Bir Başkasının Adının Konulması Suretiyle Eserin Dağıtılması, Yayılması ve Yayımlanması: Bir eserin, icranın, fonogramın veya yapımın, tanınmış bir başkasının adının kullanarak çoğaltılması, dağıtılması, yayılması veya yayımlanması da manevî haklara yönelik bir suçtur. Böylelikle başkasının adı ve ününden faydalanarak eserin hak etmediği ya da hak ettiğinden fazla bir değer elde etmesi ve/veya adı konulan kişinin şöhretinin lekelenmesi önlenmek istenmektedir.[126]

eeee. Alıntı Yapılan Kaynağın Gösterilmemesi, Yanlış, Yetersiz veya Aldatıcı Kaynak Gösterilmesi: FSEK'in 32., 33., 34., 35., 36., 37., ve 40. maddelerinde bilimsel eserlerde ya da toplumun haber alma hakkını sağlamak için yapılan yayınlarda alıntı yapılması hakkı düzenlenmiştir. İşte bu maddelerde düzenlenen hakkın bir bilişimyazılımına atıf yapılarak kullanılması ancak kaynak olan yazılımın gösterilmemesi, yanlış veya yetersiz gösterilmesi ya da aldatıcı kaynak gösterilmesi durumlarında da manevî haklara yönelik suç gerçekleşmiş olacaktır. Kişinin kendine ait bir başka eserden kaynak göstermeksizin alıntı yapması hâlinde ise

123 Dülger, s.624.
124 Dülger, s.624.
125 Dülger, s.624.
126 Dülger, s.625.

suç oluşmayacaktır. Ancak 71. maddenin 1. fıkrasının 3. bendi ile 5. bendi arasındaki fark ortaya konulmalıdır. Bir eserden yapılan alıntıda hiç kaynak gösterilmemesi hâlinde 3. bentteki hareket, yapılan alıntıda gösterilen kaynağın yetersiz, yanlış ya da aldatıcı olması hâlinde ise 5. bentteki hareket söz konusu olmaktadır.[127]

ffff. Eserin Değiştirilmesi: Son olarak yazılım sahibinin yazılı izni olmaksızın bir yazılımı değiştirme hareketi de manevî haklara yönelik bir suç oluşturmaktadır. Bu eylemle FSEK'in 16. maddesinde düzenlenen yazılımda değişiklik yapılmaması kuralı ihlal edilmektedir. Yazılımsahibi eserinin bozulmadan, değişmeden korunması ister; bu nedenle FSEK'in düzenlemesine göre yazılım sahibinin izni olmadıkça yazılımda veya yazılım sahibinin adında kısaltmalar, ekleme veya başka değişiklikler yapılması mümkün değildir. FSEK'in 16. maddesinde belirtilen sınırlar dışında yazılımda değişiklik yapılması, yazılım sahibinin yazılı iznine bağlıdır; bu iznin olmaması durumunda, yazılımda değişiklik yapılması eylemi inceleme konusu suçu meydana getirecektir.[128]

bbb. Maddî Haklara Yönelik Hareketler:

aaaa. Eserin İşlenmesi: Bir yazılımın hak sahibinin yazılı izni olmaksızın işlenmesi eylemi maddî haklara yönelik suç tipini oluşturmaktadır. Bu eylemle FSEK'in 21. maddesinde düzenlenen yazılımı işleme hakkı ihlal edilmektedir. Bir yazılımı işleme yetkisi yalnızca yazılımsahibine aittir, bu konuda yazılım sahibinden izin alınmadan yazılımın işlenmesi yoluyla, "işleme bir yazılımın" oluşturulmasıyla suç gerçekleşmiş olacaktır.[129]

bbbb. Eserin Çoğaltılması: Bir yazılımın, hak sahibinin yazılı izni olmaksızın çoğaltılması eylemi maddî haklara yönelik diğer bir suç tipini oluşturmaktadır. Çoğaltma, topluma sunulan bir yazılımın, ekonomik getiri amacıyla herkese ulaştırılması için sayılarının arttırılmasını sağlayan ve bilişimsistemleriyle yapılan teknik bir işlemdir. Bu eyleme uygulamada çok sık rastlanmakta ve bu nedenle yazılım endüstrisinde milyon dolarla ifade edilen kayıpların olduğu belirtilmektedir. Çünkü bilişim yazılımlarının yaratılması için gerekli olan emek ve ekonomik maliyet büyük boyutlardayken, kopya nüshaların hazırlanması için oldukça az zaman ve masraf yeterli olmaktadır. Bu eylemle FSEK'in 22. maddesinde düzenlenen yazılımı çoğaltma yetkisi ihlal edilmektedir. Bir yazılımı çoğaltma yetkisi yalnızca yazılım sahibine aittir, bu konuda yazılım sahibinden izin alınmadan yazılımının her ne şekilde olursa olsun çoğaltılmasıyla suç gerçekleşmiş olacaktır. Çoğaltma eyleminin asıl yazılım ya da işleme niteliğindeki yazılım üzerinde olması suçun oluşmasını etkilemeyecektir. Eserden ekonomik olarak yararlanmanın en eski ve yaygın yolu olan çoğaltma hakkı, günümüz fikri haklarının temelini de oluşturmaktadır.[130]

cccc. Eserin Failin Kendisi Tarafından Çoğaltılmış Kopyalarının Satışa Çıkarılması: Bir yazılımın ya da işlemelerinin hak sahibinin yazılı izni olmaksızın failin kendisi tarafından çoğaltılmış kopyalarının satışa çıkarılması eylemi de maddî haklara yönelik suç oluşturacaktır. Satışa çıkarmayla kastedilen yazılımların her türlü pazarlama yöntemiyle tüketicilere ulaştırılması eylemidir. Nitekim Yargıtay da buradan hareket ederek kiralamayı da tüketicilere ulaştırma

127 Dülger, s.625.
128 Dülger, s.625.
129 Dülger, s.626.
130 Dülger, s.626.

kabul ederek suçun oluştuğunu kabul etmiştir. Bu eylemle FSEK'in 23. maddesinde düzenlenen yazılımı yayma hakkı ihlal edilmektedir. Bir yazılımı satışa çıkarma hakkı yalnızca yazılım sahibine aittir, bu konuda yazılım sahibinden izin alınmadan yazılımın satışa çıkarılmasıyla suç gerçekleşmiş olacaktır.[131]

dddd. Eserin Kiralama veya Kamuya Ödünç Verilmesi Suretiyle Yayılması: Bir yazılımın hak sahibinin izni olmaksızın kiralanması veya kamuya ödünç verilmesi suretiyle yayılması hareketi de maddî haklara yönelik suç tipini oluşturacaktır. Bu eylemle FSEK'in 23/3. maddesinde düzenlenen yazılımı kiraya verme ve kamuya ödünç verme hakkı ihlal edilmektedir. Bir yazılımı kiralama ve ödünç verme hakkı yalnızca yazılımsahibine aittir, bu konuda yazılım sahibinden izin alınmadan yazılımın kiralanması veya kamuya ödünç verilmesiyle suç gerçekleşmiş olacaktır.[132]

eeee. Eserin İthal Edilmesi: Bir yazılımın hak sahibinin izni olmaksızın ithal edilmesi eylemi de maddî haklara yönelik suç tipi olarak düzenlenmiştir. Bir yazılımın ithalatı yalnızca yazılım üzerinde hak sahibi olan kişinin izniyle olabilir. Yazılım üzerinde hak sahibi olan kişiden izin alınmadan yazılımın ithal edilmesiyle suç gerçekleşmiş olacaktır. İthalat vergilerinin ödenmesi suçun oluşumunu etkilemeyecektir. İthal edilen yazılımları pazarlayan ve şahsî kullanım amacı dışında satın alan veya kullanan kişiler de aynı eylemi gerçekleştirmiş gibi kabul edilecektir.[133]

ffff. Eserin Temsil Edilmesi: Maddî haklara tecavüz suçunu oluşturan eylemlerden bir diğerini de "temsil etme" eylemi oluşturmaktadır. Zîra FSEK'in "temsil hakkı" başlıklı 24. maddesinin 1. fıkrasında *"Bir eserden, doğrudan doğruya yahut işaret, ses veya resim nakline yarayan aletlerle umumî mahallerde okumak, çalmak, oynamak ve göstermek gibi temsil suretiyle faydalanma hakkı münhasıran esersahibine aittir."* denilmek suretiyle bu hak düzenlenmektedir. Temsil hakkı, bir eserin yayım dışında başka yöntemlerle duyulara hitap edecek şekilde kamuya sunulma yetkisidir. Temsilde bir eserin sabit olmayan bir araçla kamuya sunulması söz konusu olmaktadır. Temsil, bir eserin insan duyularına hitap etmek üzere doğrudan doğruya insan algılamasına yönelirken, yayım ise eserin sabit bir ortamda kamuya sunulması şeklidir. Buna göre bir eserin topluma okunması, bir musiki eserinin icrası, bir tiyatro ya da opera eserinin seyirciler önünde oynanması ya da bir sinema eserinin izlettirilmesi temsilin içinde yer almaktadır. İşte bu tür hareketler de FSEK'in 71/1-1. maddesindeki *"bir eserin hak sahibi kişilerin yazılı izni olmaksızın temsil edilmesi"* ile suç hâline getirtilmiştir.[134]

gggg. Eserin Veriİletim Ağı Üzerinden Yayılması ve Yayımlanması: Maddî haklara yönelik suçu oluşturan eylemlerden biri de bir yazılımı hak sahibinin yazılı izni olmaksızın very iletim ağı üzerinden yaymak ya da yayımına aracılık etmektir. Bu hareketle FSEK'in 25. maddesinde düzenlenen yazılımı işaret, ses ve/veya görüntü nakline yarayan araçlarla topluma iletim hakkı ihlal edilmektedir. Bir yazılımı satışa bu şekilde iletme hakkı yalnızca yazılımsahibine aittir, bu konuda yazılım sahibinden yazılı izin alınmadan yazılımın iletilmesiyle suç gerçekleşmiş olacaktır. Bu hak, fikir ve sanat eserlerinin radyo, televizyon, uydu ve kablo gibi telli telsiz yayın

131 Dülger, s.627.
132 Dülger, s.627.
133 Dülger, s.627.
134 Dülger, s.628.

yapan kuruluşlar ile internetgibi sanal ağlar aracılığıyla kamuya sunulmasını ifade etmektedir.[135]

hhhh. Eserin Ticari Amaçla Satın Alınması: Maddî haklara yönelik suçu oluşturan eylemlerden biri de bir yazılımın hak sahibinin yazılı olmaksızın ticari amaçla satın alınmasıdır. Suç tipinde yer alan bu hareketle eser sahibinin herhangi bir mali hakkı doğrudan koruma altına alınmamaktadır. Ancak bu hareketin suç hâline getirilmesi ile hak sahibi kişilerin eserden kaynaklanan mali haklardan yararlanabilme ve bu hakları ne suretle olursa olsun belirleyebilme hakkının dolayısıyla da olsa korunması amaçlanmaktadır. Bu hareketin ticari amaçla olmayıp kişisel amaçla alınması hâlinde(ki günlük yaşamda genel olarak görülen ve eserlerden hak sahiplerinin maddî yarar elde etmesini sağlayan işlem budur) ise suç oluşmayacaktır.[136]

ıııı. Eserin Kişisel Amaç Dışında Bulundurulması ve Depolanması: Kişisel amaç dışında elinde bulundurmak ya da depolamak hareketlerinin suç olarak düzenlenmesi ile özellikle 4110 sayılı Yasa ile amaçlanan fikir ve sanat eserlerinin hukuk dışı ticareti veya buna neden olacak eylemler sonucunda hak sahiplerinin mali haklarına yönelik tecavüz eylemlerinin önlenmesi amaçlanmaktadır.Yasa koyucu kişisel amaç dışında bulundurmak ya da depolamak hareketi ile fikir ve sanat eserlerinin hukuk dışı ticarete konu olmasını kast etmektedir. Nitekim ticari amaç dışında bulundurmak veya depolamak dışındaki bütün bulundurma veya depolama hareketleri kişisel amaç içinde yer alacak ve suç oluşturmayacaktır. Ayrıca bilişim teknolojilerinin gelişimine paralel olarak depolama hareketi, mp3, mpe4, DVD, DivX ve benzeri formatlardaki verilerin toplanmasını yani kaydedilebilir, depolanabilir bir ortamda bulunmasını da kapsamaktadır.[137]

ccc. Bağlantılı Haklara Yönelik Hareketler:

FSEK'in 71. maddesi başlığı *"bağlantılı haklara tecavüz"* ibaresini içermekte ve maddenin tamamına hitap edecek şekilde madde metninin girişinde maddede yer alan bütün suçlar bakımından bağlantılı haklara tecavüzden bahsedilmekte ise de, bağlantılı hak sahipleri eser sahibisıfatına haiz olmadıklarından kendileri bakımından, icracı sanatçılar hariç, eser sahibine tanınmış bulunan manevî haklara yönelik suçlar söz konusu olamaz. Bağlantılı haklara yönelik tecavüz suçları esasen bağlantılı hak sahiplerinin mali haklarını ihlal ettiğinden doğal olarak gerçekleşen tecavüz eylemleri mali haklara tecavüz suçlarının başka bir şeklini oluşturmaktadır. Bu nedenle mali haklara tecavüz suçları için yukarıda yapılan açıklamalar bağlantılı haklara tecavüz suçu açısından da geçerlidir. Dolayısıyla bağlantılı haklara yönelik tecavüz suçları icracı sanatçılar, fonogram yapımcıları, radyo – televizyon kuruluşları ve film yapımcıları bakımından ancak FSEK'in 71. maddesinde yer alan hak sahibinin mali haklarına tecavüz suçunu oluşturan eylemler bağlantılı haklara tecavüz suçunu oluşturabilecektir.[138]

c. Tipikliğin Manevî Unsuru

FSEK'in 71. maddesinde düzenlenen her üç suç da ancak kasten işlenebilir,

135 Dülger, s.628.
136 Dülger, s.628.
137 Dülger, s.629.
138 Dülger, s.629.

yasada açıkça belirtilmediği için bunların taksirle işlenmesi mümkün değildir. Bunun dışında bu suçlar manevî unsur açısından bir özellik göstermemektedirler.[139]

d. Hukuka Aykırılık Unsuru

Failin FSEK'e göre suç oluşturan eylemleri bir rızaya dayanarak gerçekleştirdiği hâllerde suç oluşmayacaktır, çünkü her üç suç tipinde de suçun oluşması için failin eylemlerini hak sahibinin izni olmadan yapması aranmıştır.Rızanın varlığı hâlinde bu hukuka aykırılık ortadan kalkacaktır. Ancak FSEK'in 71. maddesinin 1. fıkrasında düzenlenen suçlar açısından hukuka aykırılığı ortadan kaldıran rızanın yazılı olması aranmaktadır. Buna göre bir eseri "işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticari amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan" kişinin bu hareketleri ancak yazılı izinle yapması hâlinde rızaya dayalı hukuka uygunluk nedeni söz konusu olacak ve suç oluşmayacaktır. 71. maddenin 2., 3., 4., 5. ve 6. fıkralarında yer alan suçlar ve bu suçları oluşturan hareketler açısından yazılı izin şartı gerekli görülmemiştir. Dolayısıyla bunlar açısından rızanın yani iznin sözlü olarak verilmesi ya da imzalı olmayan bir yazı ile verilmesi ancak bunun tanık vb. gibi delillerle ispat edilebilmesi halinde söz konusu rıza bir hukuka uygunluk nedeni olarak geçerli olacaktır.[140]

e. Suçun Özel Görünüş Biçimleri

aa. Teşebbüs: FSEK'in 71. maddesinde düzenlenen suçlar yukarıda da belirtildiği üzere ayrıca bir neticenin aranmadığı sırf hareket suçlarıdır. Failin hareketiyle suç da tamamlanacağı için pek çok olayda suçun teşebbüs aşamasında kalması mümkün olmayacaktır. Ancak hareketin parçalara bölünebildiği durumlarda suçun teşebbüs aşamasında kalması mümkündür. Örneğin failin elinde olmayan nedenlerden ötürü elektrik kesilmesi ya da mağdurun sistemini kapatması gibi bir nedenle hareketin yarıda kalması veya çoğaltma yapılamadan baskı sırasında zabıta tarafından kopyalama araçlarına el koyulması gibi durumlarda suç teşebbüs aşamasında kalacaktır.[141]

bb. İştirak: İnceleme konusu suçlar açısından iştirakin her hâlinin gerçekleşmesi mümkündür. Suça iştirakte TCK'nın 37, 38, 39, 40 ve 41. maddelerinin somut olayın özelliğine göre uygulanması mümkün olacaktır.[142]

cc. İçtima: FSEK'in 71. maddesinde manevî haklara tecavüzmali haklara tecavüzve bağlantılı haklara tecavüz olmak üzere üç farklı suç tipi aynı madde içinde düzenlenmiştir. Bu düzenleme karmaşıklığa yol açmıştır ve en önemli etkilerinden birisini içtima konusunda göstermektedir. Zîra fail aynı madde içinde düzenlenen ancak farklı suçlara ait olan farklı hareketleri gerçekleştirmesi durumunda bir suçun seçimlik hareketlerini mi gerçekleştirmiş olacak, yoksa farklı suçları işlemiş olarak mı kabul edilecektir?

5237 sayılı TCK'nın genel gerekçesinde suç genel teorisine ilişkin yazılmış

139 Dülger, s.630.
140 Dülger, s.630.
141 Dülger, s.632.
142 Dülger, s.632.

yeni tarihli eserlerde eylem sayısı kadar suçun oluştuğu ve kaç suç varsa o kadar da ceza olması gerektiği yönündedir. 71. maddenin özellikle 1. fıkrasında farklı hukuksal değerleri koruyan farklı suçlar bir arada düzenlenmektedir. 71/1. maddede hak sahiplerinin manevi, maddî ve bağlantılı olmak üzere üç farklı hakkı korunmaktadır. Failin gerçekleştirdiği hareketler ile üç farklı hakkın ihlal edilmesi hâlinde üç farklı suçun işlenmesi söz konusu olacaktır, ihlal edilen hukuksal değer ve/veya hakkı ihlal edilen mağdur sayısı kadar suç oluşmaktadır. Bir mağdurun birden fazla hakka sahip olması hâlinde de, örneğin sanatçının hem esersahibihem de icracı sanatçı olduğu durumlarda tek bir suç değil hem mali haklara hem de manevî haklara tecavüzolmak üzere iki farklı suç bulunmaktadır ve gerçek içtima uygulanmalıdır. Eskiden 71., 72. ve 73. maddelerde düzenlenen üç farklı suç tipi yeni düzenleme ile tek bir madde ile düzenlenmiştir, ancak bu yalnızca tek suç tipi oluşturulduğu anlamına gelmemektedir. Ancak söz konusu bu suçların korudukları hukuksal değer ve suçların yöneldikleri suç konuları farklı olduğundan bu üç suçun bağımsızlığında bir değişiklik olmamaktadır. Dolayısıyla gerçekleştirilen herhangi bir eylemin manevî, mali ve bağlantılı haklara yönelik birbirinden bağımsız hakların korunmasında bu üç ayrı suçu ilgilendiren hareketlerinin aynı madde içinde düzenlenmesi seçimlik hareket oluşturmamaktadır.

FSEK'in 71. maddesinde düzenlenen suçlar açısından zincirleme suçun gerçekleşmesi mümkündür, dolayısıyla failin aynı suçu işleme kararıyla 71. maddede düzenlenen suçlardan herhangi birisini oluşturan hareketleri birden fazla gerçekleştirmesi halinde TCK'nın 43. maddesi gereğince faile arttırılarak yaptırım uygulanır. Ancak failin örneğin aynı suç işleme kararı denilemeyecek kadar uzun aralıkla yazılımları çoğaltması eyleminde artık zincirleme suçun varlığı kabul edilmemeli burada iki ayrı suçun oluştuğu düşünülerek cezaların içtimaı kuralı uygulanmalıdır. Ayrıca farklı kişilere ait eserler hakkında suç işlenmesi halinde de TCK'nın 43. maddesi uygulanmayacaktır.[143]

f. Yaptırım, Soruşturma ve Kovuşturma

Mali haklara tecavüz suçunun yaptırımı "bir yıldan beş yıla kadar hapis veya adlî para cezası" olarak belirlenmiştir.

Manevî haklara tecavüz suçu açısından ise farklı hareketler için farklı yaptırımlar öngörülmüştür. 71/1-1'de yer alan *"bir eseri hak sahibi kişilerin yazılı izni olmaksızın her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma iletmek veya yayımlamak"* ve "hak sahibi kişilerin yazılı izni olmaksızın eseri değiştirme" hareketleri açısından "bir yıldan beş yıla kadar hapis veya adlî para cezası" olarak öngörülmüştür.

71/1-4'de yer alan bir eserin muhtevası hakkında kamuya açıklamada bulunma hareketi açısından *"altı aya kadar hapis cezası"* öngörülmüştür.

71/1-2'de yer alan "başkasına ait esere kendi eseri olarak ad koyma" hareketi için "altı aydan iki yıla kadar hapis veya adlî para cezası" öngörülmüştür; bu suçun dağıtmak veya yayımlamak suretiyle işlenmesi halinde ise hapis cezasının üst sınırı beş yıl olarak belirtilmiş ve adlî para cezasına karar verilemeyeceği düzenlenmiştir.

71/1-3'de yer alan *"bir eserden kaynak göstermeksizin iktibasta bulunma hareketi"* için *"altı aydan iki yıla kadar hapis cezası veya adlî para cezası"* öngörülmüştür.

143 Dülger, s.632.

71/1-5'de yer alan *"bir eserle ilgili yetersiz, yanlış veya aldatıcı mahiyette kaynak gösterme"* hareketi için *"altı aya kadar hapis cezası"* öngörülmüştür.

Bu suçun soruşturulması ve kovuşturulması FSEK m.75/1 gereğince şikâyete bağlıdır. Yasada suçtan zarar görenin doğrudan şikâyet etmesi yeterli görülmemiştir. Ayrıca şikâyetin geçerli olabilmesi için hak sahiplerinin veya üyesi oldukları meslek birliklerinin haklarını kanıtlayan belge ve sair delilleri Cumhuriyet Başsavcılığına vermeleri gerekir, aksi takdirde bu geçerli bir şikayet olarak değerlendirilmeyecektir.

5846 sayılı Yasanın 75. maddesinin 2. fıkrası gereğince bu yasada yer alan soruşturması ve kovuşturması şikayete bağlı suçlar için başta Milli Eğitim Bakanlığı, Kültür ve Turizm Bakanlığı yetkilileri olmak üzere ilgili gerçek ve tüzel kişiler tarafından, eser üzerinde manevî ve mali hak sahibi kişiler, şikâyet haklarını kullanabilmelerini sağlamak amacıyla durumdan haberdar edileceklerdir.

FSEK'in 71. maddesinde düzenlenen bu eylemlerin suç olarak düzenlenmesi ve yaptırıma bağlanması yanında, bu eylemler için FSEK'in 66/1. maddesi gereğince tazminat davası da açılabilecektir.

FSEK'in 76. maddesinin 1. fıkrasında *"Bu Kanun'un düzenlediği hukukî ilişkilerden doğan davalarda, dava konusunun miktarına ve Kanunda gösterilen cezaya bakılmaksızın, görevli mahkeme Adalet Bakanlığı tarafından kurulacak ihtisas mahkemeleridir."* denilmek suretiyle bu hususta ihtisas mahkemeleri kurulacağı belirtilmiştir. İstanbul, Ankara ve İzmir başta olmak üzere büyük şehirlerde bu konuda ihtisas mahkemeleri "Fikri ve Sınai Haklar Ceza Mahkemesi" olarak kurulmuş ve yasadan kaynaklanan ceza davalarına ilişkin yargılamalara bu mahkemelerde devam edilmektedir. Diğer kentlerde ise HSYK tarafından belirlenen bir aslîye ceza mahkemesi o yerde ihtisas mahkemesi olarak görev yapmaktadırlar.

Eserin Topluma Sunulması Sırasında Görülen Bilgiler ve Bu Bilgileri Temsil Eden Sayılar veya Kodların Yetkisiz Olarak Ortadan Kaldırılması veya Değiştirilmesi Suçu (m.71/2)

FSEK'e 21.2.2001 tarihli ve 4630 sayılı Yasanın 37. maddesi ile eklenen ek 4. madde ile eserin topluma sunulması esnasında kullanılan bilgiler ve bu bilgileri temsil eden sayısal kodların yetkisiz olarak ortadan kaldırılması ve değiştirilmesi yasaklanmıştır. Söz konusu Ek 4. maddede *"Eser ve eser sahibi ile, eser üzerindeki haklardan herhangi birinin sahibi veya eserin kullanımına ilişkin süreler ve şartlar ile ilgili olarak eser nüshaları üzerinde bulunan veya eserin topluma sunulması sırasında görülen bilgiler ve bu bilgileri temsil eden sayılar veya kodlar yetkisiz olarak ortadan kaldırılamaz veya değiştirilemez. Bilgileri ve bu bilgileri temsil eden sayıları veya kodları yetkisiz olarak değiştirilen veya ortadan kaldırılan eserlerin asılları veya kopyaları dağıtılamaz, dağıtılmak üzere ithal edilemez, yayınlanamaz veya topluma iletilemez. Yukarıdaki fıkra hükümleri fonogramlar ve fonogramlarda tespit edilmiş icralar bakımından da uygulanır."* denilmektedir.

FSEK'in 71. maddesinin 2. fıkrasında ise *"Bu Kanun'un ek 4 üncü maddesinin birinci fıkrasında bahsi geçen fiilleri yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlal etmeye devam eden bilgi içerik sağlayıcılar hakkında, fiilleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde, üç aydan iki yıla kadar hapis cezasına*

hükmolunur." denilmekle Ek 4. maddedeki yasağa uyulmaması suç haline getirilmiştir.

Bize göre bu suç eser sahiplerinin ve diğer hak sahiplerinin hem mali haklarını hem de manevi haklarını korumaktadır.[144]

3.3.8.2. TCK 125, 106, 105, 267, 107, 148

Her ne kadar bilişim sistemlerinin kullanılması suretiyle işlenen suçlardan bahsedilirken yukarıda altı tane suç saydıysak da bunlar tahdidi değildir. Nitekim günümüzde artık bilişim sistemlerinin kullanılması suretiyle her türlü suçun işlenmesi mümkün olabilmektedir. Hatta bu suretle cinayet dahi işlenebilmektedir. Bu bağlamda hastanede cihaza bağlı olan bir hastanın hastanenin bilişim sistemine müdahale suretiyle öldürülebilmesi ya da araçların bilişim sistemine müdahale suretiyle fren aksamının veya başka bir bölümünün işlemez hale getirilmesi suretiyle günümüzde kasten adam öldürme suçları işlenebilmektedir. Bu ayrımı yapmamızdaki amaç tek tek her suçun tanımını yapmak ve ya mevzuattaki karşılığını buraya aktarmak değildir. Nitekim bu suçların unsurları zaten bilinen bir husus olup burada tekrar bahsedilmesinin nedeni bunların da internet aracılığıyla işlenebiliyor olmalarıdır. Örneğin; BİMER'e başvuru suretiyle iftira, Facebook'da aleni hakaret, Twitter'da cinsel taciz vs. şeklinde karşımıza çıkmaktadırlar. Buna benzer şantaj ve yağma suçlarının da bilişim sistemlerinin kullanılması suretiyle işlenebildiğine artık şahit olmaktayız. Suçun unsurları yönünden herhangi bir değişiklik söz konusu olmamakla birlikte gerek kollukta gerekse savcılık ve mahkemelerde iş bölümü açısından bu durum önem arz etmekte olup içinde internet kelimesi geçen her suçun bilişim bürolarına gönderilmesi suretiyle uygulamada ciddi mağduriyetlere sebebiyet verildiği hususu vurgulanmak istenmiştir. Kanaatimize göre kolluk yada savcılıklarda bilişim büro kurulacaksa bu büronun hangi suçlara bakacağı açıkça belirtilmelidir.

3.3.9. Sanal Oyun Karakterinin ve Araçlarının Çalınması

Dijital oyun dünyasındaki gelişmeler ve buna bağlı olarak kullanıcı sayısındaki artış dijital oyun pazarını tüm dünyada olduğu gibi ülkemizde de ciddi şekilde büyütmüştür. Bu gelişmenin mutlak suretle bilişim suçları alanına yansımaları da kaçınılmazdır. Dijital oyun hesaplarının, karakterlerinin , karakter özellikleri ve oyun eşyalarının çalınması bilişim suçlarında yeni bir alan olarak karşımıza çıkmaktadır.

Uygulamada online oynanabilen oyunlarla ilgili adlî makamlara yapılan müracaatlarda genellikle ilgililerin maruz kaldıkları eylemi hırsızlık olarak nitelendirdikleri, oynanan oyunun özelliğine göre sanal dünyada yönettikleri karakterin niteliğine göre 'uzay gemimi çaldılar', 'uçağımı çaldılar', 'savaşçımı çaldılar', 'baltamı, kılıcımı çaldılar' gibi iddialarını dile getirdikleri görülmektedir. Bu tür şikayetlere konu olan olay hırsızlık mıdır? Bu sorunun cevabını verebilmek açısından klasik suçlarla ilgili tanımlar ve kavramların bilişim suçları ile ilgili sorunlarda yetersiz kaldığını ortaya koymaktadır.

Kişinin herhangi bir bedel ödemeden üye olarak dâhil olduğu ve oluşturduğu karakterle kurgulanan sanal oyun dünyasındaki hukukî statüsünün, bu dünyada sahip olduğu karakter ve bu karakterle geliştirdiği elde ettiği özelliklerin hukukî statüsünün ne olduğu halen tam olarak cevap bulmamış tartışmalı konulardır. Nerdeyse tüm online oyunlara ilk kayıt aşamasında kullanıcılara sunulan ve genellikle okunmadan onaylanan 'Kullanım Şartları Sözleşmesi' içeriklerinde oyun karakterlerinin

144 Dülger, s.633.

satılamayacağı, devredilemeyeceği ,hediye olarak dahi verilemeyeceği ,kullanıcıların oyun içerisinde sahip oldukları karakter ve eşyalarla ilgili mülkiyet hakkına ilişkin talepte bulunamayacakları *"İşbu sözleşmede aksine hükümlere bakılmaksızın, kendi hesabınızda herhangi bir mülkiyete veya sair mülkiyet haklarına sahip olmayacağınızı ve ayrıca hesaptaki tüm hakların sadece ..... games'e ait olduğunu ve olacağını ve sadece ..... games menfaatine hüküm ifade ettiğini ve edeceğini de kabul ve teyit ediyorsunuz. .... puanları veya sanal kalemler için teklif edilen veya ödenen bedel ne olursa olsun edindiğiniz oyun varlıklarında, sanal kalemler veya ..... puanlarında herhangi bir talebiniz, hak, menfaat, mülkiyet veya sair özel haklarınızın bulunmadığını kabul ve teyit ediyorsunuz. ayrıca ..... games, ilgili kanunda müsaade edilen en son dereceye kadar, hesabınızın feshi veya sona ermesi üzerine oyun varlıklarının, sanal kalemlerin veya ..... puanlarının silinmesi dahil ancak bununla sınırlı olmaksızın oyun varlıklarının, sanal kalemlerin veya ..... puanlarının imha edilmesinden, silinmesinden, değiştirilmesinden, zarara uğratılmasından, "korsanların eline geçirilmesinden" veya sair hasar veya zararlardan dolayı hiçbir şekilde mesul olmayacaktır."* şeklinde düzenlenen ifadelerle belirtilmektedir.

Kullanıcıların mevcut sözleşmeler çerçevesinde online oyun sisteminde sadece kullanım haklarının varlığından söz edilebilir olduğu değerlendirilmektedir. Ayrıca her ne kadar sözleşme hükümlerinde yasaklanmışsa da online oyunların kendi kullanıcıları arasında karakterlerinin ve oyun eşyalarının bir bedel karşılığı alım-satım, takas vb. şekilde el değiştirmesi suretiyle ekonomik değerlerinin oluşması önlenememektedir.

Konuyu ceza hukuku açısından değerlendirmek gerekirse;

Hırsızlık suçunun tanımlandığı,

"Madde 141 - *Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan kimseye bir yıldan üç yıla kadar hapis cezası verilir."* Düzenlemesinde, hırsızlık suçunun konusunun ancak taşınır bir mal olabileceği açıkça belirtilmiştir.

Bu hâlde online oyun karakterinin ve oyun eşyalarının taşınır bir mal olarak kabulü mümkün müdür? Bu konudaki tartışmalar bilişim sistemindeki verilerin taşınır mal niteliği taşımadığı ve hırsızlık suçunun konusu olamayacağı ile verinin bilişim sisteminde karşılığı olan ve gerçek dünyada ekonomik değer ifade eden varlığının hırsızlık suçuna konu olabileceği şeklindedir.

Birinci görüşe göre online oyun karakterlerinin hukuka aykırı olarak ele geçirilmesinin 5237 sayılı yasanın 243 ve 244. maddelerinde düzenlenen bilişim sistemine girme ve sistemi engelleme , bozma, verileri yok etme veya değiştirme suçlarının konusu olabileceği ifade edilmektedir.

Sonuç olarak online oyun sistemlerinin bir bilişim sistemi olduğunda tartışma bulunmamaktadır. Kullanıcıların kendilerine tanınmış hak ve yetki kapsamında erişim sağlayarak kullandıkları sistemdeki karakterlerine, kullanıcıya ait şifrenin ele geçirilerek yetkisiz erişim yapılması TCK 243 maddede düzenlenen suçu oluşturduğu ifade edilmektedir.

Yetkisiz erişim yapılarak kullanımı sağlanan oyun karakterine ait şifrenin

değiştirilmesi , tamamen kullanıcıya ait kaydın silinmesi , oyun karakterine ait özelliklerin başka karakterlere aktarılması, oyun karakteri ve oyun eşyalarının maddî veya manevî bir menfaat karşılığı el değiştirmesi TCK'nın 244 maddesinde tanımlanan bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması suçunu ve bu fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması suçunu oluşturduğu ifade edilmektedir.

İkinci görüşe göre ise online oyun karakterlerine ve oyun eşyalarına yönelik yukarıda ifade edilen eylemlerin 5237 sayılı TCK'nun 142/2-e maddesindeki bilişim sistemleri kullanılması suretiyle hırsızlık suçunu oluşturacağı ifade edilmektedir.

Konu hakkında uygulamanın ne şekilde gelişeceği klasik suç tanımlarındaki kavramların artık günümüz şartlarına uygun yorumlanarak mevzuatımıza dahil edilmesi ile de ilgilidir. Sanal dünyada işlenen gerçek suçların sayısı her geçen gün hızla artmaktadır. Yeni suç tiplerine de ihtiyaç duyulması zaman içerisinde kaçınılmazdır.

4 DELİL ELDE ETME YÖNTEMLERİ

4. DELİL ELDE ETME YÖNTEMLERİ

4.1.1. İfade Alma

4.1.2. Müştekiden Talep Edilecek Bilgiler

Suç nedir? Suçun konusu ve boyutu hakkında müştekinin bilgisi hakkında sorulara cevap aranır. Varsa suç delilleri nelerdir, internet site bilgisi, ekran çıktıları, e posta iletilerihakkında bilgi alınır.

Suç ne zaman işlenmiştir? Suçun hangi tarihte, hangi saatte işlendiği hakkında tam olarak bilgi edinilmelidir.İnternet ortamında işlenen suçlarla şüpheliye ulaşmak için zaman IP bilgisinin doğru tespiti açısından önemlidir.

Suç nerede işlenmiştir? Hangi internet sitesi, iletişim platformu ve dijital metaryal, bilgisayar kullanılarak işlenmiştir sorularına cevap aranır.

Suç nasıl işlenmiştir? İnternet suçlarında yazılı, görüntülü, sisteme uzaktan müdahale edilerek mi veya bilişim sistemleri kullanılarak mı işlendiğine dair cevap aranır.

Suç neden işlenmiştir? Müştekiden menfaat talep etmek, kişisel ve ailevi nedenler, siyasi ve fikrî nedenler vs. soruşturulur.

Suçu kim işlemiştir? Şüpheli şahsın açık adres ve kimlik bilgisi, bilmiyorsa şüpheliyi tespit etmekte kullanılabilecek e posta hesap adı, IP numarası, telefon numarası, profil adı, link sayfası, internet sitesi, ID numarası, irtibat numaraları gibi bilgiler müştekiden talep edilir.

4.1.3. Şüpheli İfadesinde Sorulacak Bilgiler

Şüpheli şahsın ifade alma yönetmeliğine göre kimlik bilgileri ve iletişim bilgileri tutanağa geçirilir.Suçu ne zaman, hangi bilgisayar ve iletişim cihaz ve materyalleri kullanarak işlendiği öğrenilir. Müştekinin iddia ettiği olayı gerçekleştirip gerçekleştirmediği, e posta, profil adının, IP numarasının kayıtlı olduğu telefon aboneliğinin kendi üzerine kayıtlı olup olmadığı, suçlamayı kabul etmiyorsa iddia edilen suçu kimin işlemiş olduğu hakkında bilgisi, arama kararı alınmışsa dijital delillerin incelenmesinde tespit edilen bulgular ile ilgili sorulara cevap aranır.

4.1.4. IP Adresinin Tespiti

4.1.5. IP Adresi Nedir?

İnternet'te her bilgisayarın bir IP (İnternet Protokol) adresi vardır. Tipik bir IP adresi, noktalarla ayrılan 3'lü 4 rakam grubundan oluşur; örneğin, 212.123.234.20 şeklindedir. IP numaralarının tükenme noktasına geldiği günümüzde yeni bir IP versiyonu olan IPv6; 340 trilyon kere trilyon kere trilyon adet farklı IP adresi sağlamaktadır.

Bir bilgisayarın IP adresi varsa, İnternet üzerindeki tüm bilgisayarlar bu adresi kolayca bulur. Yani bir sitenin IP adresini biliyorsanız, Web tarayıcınıza bu adresi

yazarak da bağlanabilirsiniz. Ancak bu rakamları akılda tutmak zor olduğundan her bir IP adresine karşılık gelen alan adları verilmiştir. Çoğu İnternet Servis Sağlayıcılarda bulunan özel sunucu bilgisayarlardan (Alan Adı Sunucuları - Domain Name Server-DNS) oluşan bir ağ, hangi alan adının hangi IP adresine karşılık geldiği bilgisini tutar ve kullanıcıları doğru adreslere yönlendirir. İnternette trafiğin işlemesi bu IP adreslerine bağlıdır. Böylece hiçbir karışıklık olmaz.

Sizin bilgisayarınızın da bir IP adresi vardır. ISS'nize telefon numarasını çevirip bağlandığınızda, aslında o ISS'de yer alan bir sunucu bilgisayara bağlanıyorsunuz demektir. Bu sunucu bilgisayar, bağlantı sırasında kullandığınız kullanıcı ismi ve şifrenize göre elindeki boş adreslerden birini (örneğin 212.172.xxx.xxx gibi) İnternet Protokolü (IP) numarasını bilgisayarınıza atar.

Bu yüzden her bağlantıda IP adresinizin son numarası değişir. Ancak IP numaranız değişse bile sunucudaki LOG kayıtlarında hangi tarihte ve saatte hangi IP adresinin hangi telefon numarasına tahsis edildiği saklanır.

Artık internette dolaşırken sizin kimliğiniz aldığınız IP numaranızdır. Siz de Web sitelerine, e-posta kutularına bağlanırken size atanmış olan bu IP adresini kullanırsınız.

Bazı IP adresleri sabittir (static IP), yani IP adresleri hiç değişmez. Bir Web sitesinin adresi her yazıldığında bulunabilmesi için IP adresi genellikle sabittir.

Kendi IP adresinizi, İnternet'e bağlıyken **www.ipnedir.com** veya **www.whatismyip.com** isimli sitelere girerek öğrenebilirsiniz.

Herkesçe kabul edilmiş bir İnternet adresleme sistemi. Merkezi ABD de olan ICAAN adlı kuruluş tarafından verilen IP adresleri sayesinde aynı adresin birden fazla makinaya verilmesi önlenmiş oluyor. **www.iem.gov.tr** gibi harflerle ifade dilmiş bir adres aslında rakamlardan oluşur, Örneğin; **http://www.iem.gov.tr** adresi aslında 212.175.85.227 rakamlarına karşılık gelir.

4.1.6. Whois Bilgisi ve IP numarası Tespiti

Whois sorgusu ile internet sitesi hakkında birtakım (site yetkilisi, yer sağlayıcısı, site içeriği) bilgilere ulaşabiliriz.

Whois bilgilerine ücretsiz olarak hizmet veren siteler bulunmakla birlikte Telekomünikasyon İletişim Başkanlığının resmi internet sitesi olan **www.tib.gov.tr** isimli internet sitesinde bulunan İnternet Site Bilgisi Sorgulama ekranından internet siteleriyle ilgili birtakım bilgileri temin etmek mümkündür.

Whois sorgusu neticesinde elde ettiğimiz bilgiler ile ilgili firmadan sitenin yayın yaptığı adres bilgisi, içerik sağlayıcı şahıs veya firma bilgisi, kimlik ve adres bilgisi gibi taleplerinde bulunabiliriz.

4.2. E-Posta Bilgilerinin Analizi

4.2.1. Elektronik Posta Başlık Bilgilerini İnceleme

Header bilgisi kullandığımız mail servislerinden (Hotmail, Windowslive, Outlook.com, Msn, Gmail, Yahoo, Mynet) herhangi birine gelen mailin gönderici bilgilerinin detaylı şekilde belirtildiği ve mailin gönderildikten sonra izlediği yolu görmemizi sağlayan bir bilgidir. Bu sebepten dolayı mail header bilgilerini mail göndericisinin maili gönderirken kullanmış olduğu IP numarasını ve gönderdiği tarih ve saati ile birlikte tespit etmemiz genellikle mümkün olmaktadır. Servis sağlayıcılarının header bilgileri birbirinden farklılık göstermektedir. Burada önemli olan bir diğer husus ise tespit ettiğimiz IP numarasının gönderilme tarihidir. Bu tarih çoğunlukla Türkiye dışında bir zaman dilimine ait olduğundan bu tarih ve saat Türkiye zaman dilimine çevrilmelidir. Ayrıca Gönderilen eposta içeriğinde IP bilgilerinin gönderici tarafından gizlenmiş olabileceği de göz ardı edilmemelidir. Bu durumda ilgili eposta servis sağlayıcı firmadan yazışma ile IP numarası talep edilmelidir.

4.2.2. Elektronik Posta Hesap Detay Bilgilerinin Talep edilmesi

Elektronik posta hesap detay bilgileri şahısların mail hesabını hangi tarihte açtığı, hesabını ilk açtığı tarih ve saatte hangi IP numarası ile kayıt olduğu, kayıt olduğu esnada mail servisine vermiş olduğu kişisel kayıt bilgileri ve mail hesabında kayıtlı bulunan kişi listesi ihtiyaca göre istenmektedir.

4.2.3. İnternet Soruşturmalarında Dikkat Edilecek Hususlar

a. İnternet üzerinden işlenen suçlarda dikkat edilecek en önemli husus, şikâyete bağlı olan suçlarda mutlaka Cumhuriyet Savcılığının talimatı olması gerektiğidir. Kurumlar, Savcılık talimatı olmadan IP'nin kimin tarafından kullanıldığıyla ilgili bilgi vermemektedirler.

b. IP tespitlerinde, saat bilgisinin doğru tespit edilmesi ve ülke saatine doğru olarak çevrilmesi şüphelinin tespiti açısından önemlidir.

c. Ülkemizde yayın yapan ve kayıtlı olan internet sitelerinin sahibi olan firmalardan, içerik ve yer sağlayıcı firmalardan her türlü bilgi ve belge talebinde bulunulabilir. Ancak ülkemizde kayıtlı olmayan yurt dışı kaynaklı firmalardan ancak adlî istinabe yolu ile savcılık makamı talepte bulunabilir. Ancak, yurt dışı kaynaklı olup ülkemizde temsilciliği bulunan firmalardan emniyet birimleri talepte bulunabilir. Ülkemizde temsilciliği olan tek firma Microsoft Corporation firmasıdır.

d. Aramada esnasında tespit edilen dijital materyallerin imajlarının(kopyalarının) alınarak incelenmesinde kullanılmak üzere, ilgili Cumhuriyet Savcılığı'ndan, el konulan materyallerin kapasitesinden %30 fazla kapasiteli harddisk talebinde bulunulur. Örneğin el konulan materyallerin kapasitesi 500 GB ise imaj alınmak için kullanılacak harddisk 750 GB kapasiteli olmalıdır.

e. IP bilgisi istenen firma, kendi hizmet sağladığı ülkenin zaman dilimine göre tarih ve saati bildireceğinden, tespit edilen IP bilgilerinintarih ve saatinin ülkemiz saatinde olup olmadığının kontrol edilmesi gerekir. Türkiye, zaman dilimi olarak yaz saati uygulamasında GMT +3, kış saati uygulamasında ise GMT +2 zaman dilimini

kullanmaktadır. GMT -7, UTC -7 ve -07 şeklinde verilen bilgilerdeki **zaman dilimi bilgisi aynıdır ve zaman dilimi -7 dir.** Verilen satin ülkemiz değerindeki saate çevirebilmesi için öncelikle -7 zaman dilimi ile ülkemiz zaman dilimi arasındaki saat farkını tespit edilmesi gerekmektedir. Buradan yola çıkarsak GMT -7 ile GMT +2 arasındaki saat farkının 9 saat olduğu açıkca görülmektedir. Yani gönderilmiş olunan saat bilgisine 9 saat ekleyerek bu saate ülkemizde denk gelen saat tespit etmiş olunur.Sonuç olarak gönderilen tüm IP saatlerinin ülkemiz zaman dilimine çevrilmesi gerekmektedir. Yukarıdaki örnekte belirttiğimiz gibi, GMT-7 zaman dilimini GMT +2 ye çevirmek için 9 saat eklememiz, yine GMT +8 zaman dilimini GMT +2 ye çevirmek için ise 6 saat çıkarmamız gerekmektedir.

4.3. Arama ve El Koyma

4.3.1. Arama ve El Koyma Kararı

Bilgisayar, bilgisayar kütükleri ve programlarında arama el koyma işlemi yapılabilmesi için öncelikle şüphelinin kullanımında ki cihazların tespiti ve elde edilmesi amacıyla CMK 116 ve devamı maddeleri gereğince genel anlamda arama kararı ile birlikte CMK 134 kapsamında elde edilecek materyallerin incelenmesi mahkemeden talep edilmelidir.

Bilgisayar, bilgisayar kütükleri ve programlarında arama el koyma işlemi CMK'nın 134. maddesi ile Adlî ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde düzenlenmiştir. Bu düzenlemelere göre "Bir suça ilişkin soruşturma sırasında başka surette delil elde edilmesi imkânı yok ise, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, kayıtlardan kopya çıkarılmasına, kayıtların çözülüp metin hâline getirilmesine hâkim tarafından karar verilir" (CMK m. 134/1; Yön. 17/1). Bu düzenlemeye göre bilgisayar, bilgisayar kütükleri ve programlarında arama yapılabilmesi için aşağıdaki şartlar bulunmalıdır:

- Suç soruşturması olması,
- Başka surette delil elde etme imkânı bulunmaması,
- Şüphelinin kullandığı bilgisayar veya bilgisayar programı/kütüğü olması,

Bilgisayar kavramının gelişen teknolojiye uygun olarak geniş yorumlamak gerekir. TDK bilgisayarı, "Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin." Olarak tanımlamıştır. Kişisel bilgisayarların dışında kullanılan cep telefonları, tablet bilgisayarlar, akıllı televizyonlar, harici hard diskler, flash diskler, hafıza kartları, oyun konsolları, medya oynatıcıları, navigasyon cihazları, CD ve DVD'ler vb. otomatik işlem yapan ve veri depolayabilen tüm cihazların bu kapsamda değerlendirilebilir.

- Cumhuriyet Savcısının talebi olması,
- Hâkim tarafından karar verilmesi,

El koyma işlemi kararı olay yerinde bulunan kolluk tarafından, CMK 134/2 maddesinde belirtilen gerekçeler göz önünde bulundurularak bir tutanakla tespit edilerek uygulanır. Bu nedenle bilgisayardaki verilerin mevcut hâli ile yedeği alınmalı, bilgisayar iade edilmeli ve yapılacak arama işlemi bu yedek üzerinde yapılmalıdır. Şifre çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar

gecikme olmaksızın iade edilmelidir. Bizzat bulundurulması suç olan kredi kartı şifreleri, çocuk pornografisi vb. yedekler verilmemelidir.

Çıkartılacak yedekten şüpheliye veya vekiline örnek verilmesi bu kişilerin isteğine bırakılmıştır. Ancak şüpheliye örnek isteyip istemediği sorulup bu husus kayıt altına alınmalıdır.

CMK'nın 134/5. Maddesinde düzenlenen sistemdeki verilerin tamamının veya bir kısmının kopyası alınıp veriler kâğıda yazdırılarak bu hususun tutanağa geçirilmesi uygulaması bilişim araçlarının niteliği, barındırdıkları verilerin büyüklüğü düşünüldüğünde amaca hizmet etmediğinden uygulama imkânı bulunmamaktadır.

4.3.2. Olay Yerinde Arama

Bilişim suçlarında delil toplama konusu, bu suçların en önemli sorunlardan birisini oluşturmaktadır. Delil toplamadaki başarı oranı, bilişim suçlarıyla mücadelenin önemli bir göstergesidir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz saptanması ve zarar görmeden toplanması, ilk olay yeri müdahalesinin düzgün yapılmasıyla mümkündür.

Bilişim suçlarında, suçun iz ve eserlerinin bulunabileceği yerler iyi bilinmeli; pek çok olasılık üzerinde titizlikle durulmalıdır. Delil elde etme çalışması sırasında, olay yerinde varsa (örneğin güvenliği sağlayan) konu hakkında bilgi ve tecrübesi olmayan kişilerin aygıt ve sisteme müdahaleleri kesinlikle engellenmelidir. Yanlış bir müdahalenin, delilleri tümüyle yok edebileceği gözden uzak tutulmamalıdır.

Elektronik delillerin elde edilme aşaması, klasik suçlarda olduğu gibi kolluğun olay mahalline intikaliyle başlar. Yine klasik suçlarda olduğu gibi olay mahallinin güvenliğinin sağlanması, yetkisiz kişilerin olay yerinden çıkarılması gibi uygulamaların derhal yerine getirilmesi çok önemlidir. Olay yerinde bulunan elektronik aygıtların durumlarının sağlıklı bir biçimde korunabilmesi ancak bu sayede sağlanabilir.

Ancak olay yerinde dijital delillerden farklı olarak klasik suç delillerinin yer alması da kuvvetle muhtemeldir. Özellikle söz konusu bir bilgisayar olunca, klavye ve fare (mouse) üzerinde bulunabilecek parmak izleri, mahalde bulunan şüpheliye ait giysiler, eşyalar vb. unsurlar da birer delildir. Bu aşamada kriminalistik inceleme de ihmal edilmemelidir. Fakat bu, hassasiyet gerektiren potansiyel dijital delillere zarar vermeden yapılmalıdır. Örneğin bir CD üzerinde yapılacak parmak izi araştırması, kullanılan kimyasallar nedeniyle CD'nin içerisindeki bilgilerin kaybını doğurabilecektir. Bu nedenle kriminal veri toplama ile adlî bilişim verileri toplama arasında makul bir denge tutturulmalıdır.

Öncelikle olay yeri fotoğraflanmalı, ortamda bulunan bilgisayar, yazıcı ve diğer donanım aygıtlarının konumları belirtilecek şekilde notlar ve krokiler hazırlanmalıdır. Özetle, bu aşamaya kadar uygulanan yöntemler açısından, kriminalistik ile adlî bilişim yöntemlerinin bir arada yürütüldüğünü söylemek mümkündür

4.4. Elektronik Delil

4.4.1. Dijital/Elektronik Delil (e-delil)

Bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen

bilgi ve verilerdir. Dijital deliller, klasik delillerden farklılık arz eder. Klasik deliller, gözle görülebilen, üzerinde el koyma, muhafaza altına alma kararı verilerek kolayca götürülebilen deliller iken; dijital deliller, bu kadar somut bir yapıya sahip değildir. Elbette ki dijital deliller de bir donanıma ihtiyaç duyar dolayısıyla bir dijital delilin içerisinde bulunduğu bir donanım aygıtı mutlaka vardır. Ancak aslolan, bu donanım aygıtı içerisindeki e-delillerdir.

Dijital delil olarak elektronik aygıtlardan elde edilebilecek ve delil oluşturabilecek bulgular şunlar olabilir:

- Video görüntüleri
- Fotoğraflar
- Yazı dosyaları (word, excel, open office vb. dosyaları)
- Çeşitli bilgisayar programları
- İletişim kayıtları (SMS, MSN Messenger, GTalk vb. kayıtları)
- Gizli ve şifreli dosyalar / klasörler
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları
- Son girilen ve sık kullanılan internet siteleri
- İnternet ortamından indirilen (download) dosyalar
- Ve bu türden olup, silinmiş dosya/klasörler

4.4.2. Dijital Delil Nerelerde Bulunur?

Yukarıda da belirttiğimiz üzere dijital delil, bir elektronik aygıt üzerinde bulunur. Dijital delillerin mutlaka bir elektronik donanım içerisinde bulunabilir yapısı, klasik delillerden ayrıldığı bir noktadır. Zîra klasik deliller, herhangi bir yerde olabilir. Yine bir başka farklılık olarak bir suça ilişkin delillere herhangi bir şekilde ulaşmak mümkün olabilir iken, dijital deliller, birtakım teknik inceleme ve analiz yöntemlerine başvuru zorunluluğu doğurmaktadır. Dolayısıyla dijital delilin elde edilmesi klasik delillere nazaran çok daha zordur. Ayrıca, dijital deliller çok çabuk bozulabilmekte, değiştirilebilmekte, kaybolabilmekte ve hatta yok edilebilmektedir.

Dijital delilin içerisinde mevcut olabileceği en önemli elektronik donanımları şu şekilde sayabiliriz:

a. Bilgisayar
b. İnternet Ortamı
c. El Bilgisayarları (PDA, PALM, Pocket PC)
d. Cep Telefonları
e. Hafıza Kartları
f. Taşınır Bellekler (Flash Memory), CD ve DVD'ler
g. MP3 Çalarlar
h. Kamera ve Fotoğraf Makineleri
ı. Yazıcı, Faks ve Fotokopi Makineleri
i. Diğer Donanımlar

İçinde delil barındırabilecek ve adlî bilişim incelemesine konu olabilecek donanımlar bu sayılanlarla sınırlı değildir. Sayıları her geçen gün artmakta ve çeşitlenmekte olan ve delil ihtiva edebilecek elektronik cihazlara şunlar örnek olarak sayılabilir: Oyun konsolları, ağ cihazları (network), modemler, küresel konumlama cihazları (GPS), kredi kartı kopyalama cihazları, telesekreterler vs.

4.5. Elektronik Delil Elde Etme ve Saklama

Toplama, delillerin elde edilmesidir. Toplama aşamasında olay yeri öne çıkmaktadır. Delillerin sağlıklı biçimde toplanabilmesi, olay yerine yapılan ilk müdahalenin ne kadar sağlıklı olduğuna bağlıdır. Delil toplanması esnasında her donanımtürü için farklı bir yöntem izlenmesi gerekebilir. Adlî bilişimuzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir.

Olay yeri incelemesi, çevre güvenliğinin sağlanmasından, delillerin laboratuara ulaştırılmasına kadar olan süreci kapsar. Bu süreçte olay yerinden delillerin toplanması en temel aşamadır. Çünkü deliller ne kadar sağlıklı toplanırsa, sonraki aşamalar o kadar başarılı bir şekilde sonuçlanacaktır. Delillerin toplanması özel bir uzmanlık gerektirmektedir. Olay yeri ekipleri bilişim sistemleri konusunda yeterli bilgiye sahip olmalı ve delilleri yok edebilecek dijital bubi tuzaklarına karşı dikkatli olmalıdır. Olay yerinde elde edilen delillerin laboratuara getirilmesine kadar olan zaman diliminde delillerin bozulmadan saklanması ve laboratuara sevk edilmesi de bu süreç içerisindedir.[1]

4.6. İmaj Alma

Kriminal inceleme yürütülürken elektronik deliller de toplanmalı, bunun için öncelikle delillerin nerede ve hangi formatta olduğu, nasıl depolandığı tespit edilmelidir. (C:\Users\Documents and Settings\Aydogan Tan\Belgelerim\web\Aydogan Tan\Eski av.tr dosyalar\adlî-bilisim.html - ftn11. gibi) Sonrasında, ortamda bulunan elektronik donanımların çalışma biçimleri ve birbirlerine bağlılıkları tespit edilerek buna göre hareket edilir. Örneğin, olay yerinde kapalı konumda bulunan bir bilgisayar varsa kesinlikle açılmamalı; açık bir bilgisayar ise kesinlikle doğrudan kapatılmamalıdır. Bilgisayarın açılması hâlinde işletim sistemi çalışacak ve bilgisayar verileri işlemeye başlayacaktır. Bunun sonucu ise, verilerin üzerine yeniden veri yazılması ve potansiyel delillerin kaybı söz konusu olabilecektir. Bilgisayar açık ise kesinlikle hiçbir program çalıştırılmamalı, hatta bilgisayar kapatılmamalıdır. Herhangi bir programın çalışması, bir potansiyel delilin kaybı anlamına gelebilir. Bilgisayar çalışıyor konumda fakat ekranı siyah ise, ekranın açık olup olmadığı kontrol edilmeli, sonrasında fare (mouse) oynatılarak görüntünün gelmesi sağlanmalıdır. Çalışmakta olan bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesi, doğal olarak o anda ve olay yerinde mümkün olamayacaktır. Bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gereklidir. Ancak kapatılması dahi veri kaybına yol açabilecek bir donanımın götürülmesi durumunda öncelikle bilgisayar üzerinde bulunan ve çalışma konumundan çıkınca yok olabilecek tüm bulgular tespit edilerek belirlenmeli, kesinlikle ekran görüntüsü fotoğraflanmalı, çalışan programlar varsa not edilmeli ve bilgisayar kapatılmayarak arkadaki güç kablosu çekilmelidir. Bunun yapılması belki birtakım verilerin kaybına yol açabilecekse de, delillerin bütünlüğünün bozulmasının önüne geçecektir. Delillerin tümünün kaybındansa, az miktar verinin kaybı daha tercih edilir bir durumdur. Kaldı ki bilgisayardaki tüm delillere adlî bilişim uzmanlarınca ve laboratuar ortamında çeşitli analizler yapılmaksızın ulaşılması çok olası bir durum değildir.

Bilgisayarların muhafaza altına alınarak incelenmek üzere laboratuarlara götürülmesi de oldukça dikkat ve özen gerektirmektedir. Donanım araçlarının hassas

1 Dülger, s.669.

yapısı gereği, dikkatlice paketlenmesi ve yine aynı dikkatle taşınması şarttır. Sarsıntı, elektrik akımları, elektromanyetik ortamlar, aşırı sıcak ya da sıvı maddelerle teması, bu aygıtların işlevini yitirmesine neden olacaktır ki bu da potansiyel delillerin kaybıdır. Ayrıca paketlemenin, statik elektrikten ve manyetik alanlardan etkilenmeyecek biçimde yapılması da gerekmektedir. (C:\Users\Documents and Settings\Aydogan Tan\Belgelerim\web\Aydogan Tan\Eski av.tr dosyalar\adlî-bilisim.html - _ftn14.)

Delil araştırma amaçlı olarak yapılacak incelemeler, donanımlar üzerinde değil, alınan kopyaları üzerinde yapılacaktır. Bu, donanımlar içerisindeki verilerin kaybını önleyecektir. Bu nedenle aygıtlardaki verilerin sağlıklı kopyalarının alınması çok önemlidir. Adlî bilişimde yapılan birebir kopyalama işlemine imaj (birebir kopya) denilmektedir. Bu kopyalama, sistemdeki tüm verilerin, özel yazılımlar veya donanımlar kullanmak suretiyle ve bit-bit başka bir ortamda bir örneğinin (imajının / birebir kopyasının) oluşturulması suretiyle yapılır. Adlî imajın önemi, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşma olanağını vermesidir. İmaj alma işlemi iki şekilde icra edilmektedir;

4.6.1. Donanımsal İmaj Alma

Adlî imaj alma işlemi için özel olarak geliştirilmiş cihazlar kullanılır. Söz konusu cihazların bir girişine delil diski diğer girişine de imajın içine alınacağı disk bağlanarak işlem gerçekleştirilir. Burada delil diskinin bağlı olduğu girişin yazma korumalı olması sebebi ile delil bütünlüğünün bozulması ihtimali söz konusu değildir. İşlem sonucunda "sayısal doğrulama değeri (Hash)" üretilir.

4.6.2. Yazılımsal İmaj Alma

Donanımsal imaj almada kullanılan cihazların maliyetlerinin yüksek olması kolluk kuvvetlerini ücretsiz ve güvenilir alternatifler aramaya itmiştir. Bu kapsamda kullanılan yazılımsal imaj alma tekniklerini iki başlık altında toplayabiliriz.

a) Çalıştırılabilir CD ler (Boot CD) vasıtasıyla;
İnternet üzerinden ücretsiz olarak temin edilebilen ve delil bilgisayarına takılarak CD üzerine yüklü olan işletim sisteminin çalıştırılması ve delil disklerinin yerlerinden sökülmeksizin imajlarının alınması işlemidir. Donanımsal imaj almaya oranla daha fazla eğitim gerektirmekte olup, delil disklerine yazma korumalı olarak bağlanır ve delilin bütünlüğünün bozulması ihtimali söz konusu değildir. İşlem sonucunda "sayısal doğrulama değeri (Hash)" üretilir. En çok kullanılan adlî inceleme amaçlı hazırlanmış çalıştırılabilir CD'ler; FCCU Gnu/Linux Boot CD, Helix Boot CD, Caine Boot CD, Backtrack Boot CD vb.

b) Adlî İnceleme Yazılımları Kullanılarak;
Adlî incelemede kullanılan programların hemen hemen hepsinin imaj alma bölümü bulunmaktadır. Programın çalıştığı bilgisayara yazılımsal veya donanımsal yazma korumalı olarak bağlanması suretiyle imaj alınır. Bu işlem sonucunda da Hash değeri üretilir.

İmaj alma işleminde dikkat edilmesi gereken önemli bir başka husus da, kopyaların alınacağı sistemin, örneğin bilgisayarın, doğrudan çalıştırılmaması gerektiğidir. Bilgisayarın açılması, işletim sisteminin de çalışmasına bağlı olarak, yeni veriler işlerken önceki verilerin kaybı sonucunu doğurabilecektir.
Elektronik delillerin elde edilmesi sırasında dikkat edilmesi gereken hususlar;

a) Şüphelilerden ele geçirilmesi muhtemel delillere ait liste, arama yapacak personele verilmeli,

b) Olay yerinin güvenliği sağlandıktan sonra olay yeri detaylı fotoğraflanmalı,

c) Dijital delillerde parmak izi araması yapılabileceği göz ardı edilmemeli, bu sebeple aramaya katılan her personel mutlaka eldiven kullanmalı,

d) Kapalı bilişim sistemleri açılmamalı, açık durumdakiler ise hemen kapatılmamalı,

e) Elektronik delillere şüpheli, yakını veya vekili yaklaştırılmamalı,

f) Aramada olay yerine ilgisiz kişi veya personelin girmesine müsaade edilmemeli,

g) Alınan kopya veya el konulan malzemeler inceleme yerine güvenli şekilde sevk edilmeli,

h) İnceleme sırasında kopyaların zarar görmemesi için gerekli düzen sağlanmalıdır.

4.6.3. Saklama

Suç Eşyası Yönetmeliği'nin 9. maddesi, "Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler"i düzenlemektedir. Bu hüküm, "Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir."şeklinde düzenlenmiştir.

4.7. Şifre Çözme, Çözümleme ve Veri Kurtarma

4.7.1. Dekriptoloji (Şifre Çözme)

İnceleme sırasında şifrelenmiş dosya veya diskler ile karşılaşılması durumunda, özel yazılımlarla şifrelerin kırılması işlemi uygulanır.

4.7.2. Steganografi (Gizlenmiş Verilerin Çözümlenmesi)

Steganografi tekniği, gizli bir mesajın çeşitli yöntem ve tekniklerle açık bir mesajın içerisine gizlenmesidir. Dolayısıyla, steganografi'nin şifrelemeye göre en büyük avantajı bilgiyi gören bir kimsenin gördüğü şeyin içinde önemli bir bilgi olduğunu farkedemiyor olmasıdır, böylece içinde bir bilgi aranmamaktadır.

4.7.3. Veri Kurtarma

Arızalı veya hasar görmesi sebebiyle imajı alınamayan veri depolama aygıtlarının özel donanım ve yazılımlar vasıtasıyla imajlarının alınması işlemidir. El konulan materyal veri kurtarma işleminden sonra çalışır vaziyette olmayabilir.

4.8. Elektronik Delillerin İncelenmesi (Tanımlama)

Toplama safhası, imaj alma işlemi ile sona erer ve inceleme aşaması başlar. İmajın alınmasından sonra artık işin teknik yönü biraz geride kalmıştır. Bu safhada elde birtakım bulgular vardır. Bunların bazıları görünmekte, bazıları henüz görünmemektedir. Görünmeyen bulgulardan kasıt, gizli ve silinmiş dosyalardır. İnceleme ile tüm bu bulgular üzerinde çeşitli işlemler yapılarak olası suç unsurları

ortaya konulur. İnceleme safhası özetle, imajı alınmış verilerin gözle görünür biçime getirilme sürecidir. İnceleme aşaması sonucunda her türlü veri ortaya konulur. Örneğin; fotoğraflar, grafik dosyaları, videolar, çeşitli yazı dökümanları (word, excell, openoffice vb.), konuşma kayıtları (chat, MSN, GTalk vb.), e-postalar, ziyaret edilmiş ve sık kullanılan web siteleri, sıkıştırılmış dosya ve klasörler, şifreli dizinler, silinmiş dosya ve klasörler, dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları ilk başta akla gelen ve de en sık rastlanan hususlar olarak sayılabilir.

Bu aşamada birtakım yazılımlar kullanılmaktadır. Ülkemizde kolluk tarafından da kullanılan EnCase, X-Ways ve FTK bu yazılımlara örnek olarak verilebilir.

4.9. Elektronik Delillerin Analizi

Sistemdeki imajı alınmış verilerin tümünün gözle görünür hale getirilmesinden sonra analiz aşamasına geçilir. Bu aşamada, elde edilen verilerin hangilerinin ne ölçüde adlî makamlara sunulmak üzere raporlanacağının tespiti yapılır. Bu safhanın bir tür ayıklama aşaması olduğunu söylemek yanlış olmayacaktır. Tüm ilgisiz dosyalar bu değerlendirme aşamasında elenir ve raporlama aşamasına geçilmez; işe yarayabileceği düşünülen bulgular, elde ediliş metodlarını da ayrıntılarıyla anlatan tutanaklarla teslim edilir.

4.10. Raporlama ve Yetkili Makama Sunma

Bu aşamada, dijital deliller toplanmış, inceleme ve analiz aşamalarından geçmiş ve artık adlî bilişimin son safhası olan raporlamaya gelinmiştir. Bundan sonra yapılacak olan, hangi bulguların o soruşturma açısından kullanılabilir olduğunun belirlenerek adlî makamlara sunulmasıdır. Bu yönüyle raporlama safhası, hukukî bir değerlendirmeyi içermektedir. Ancak burada başka bir soru akla gelmektedir: Bu hukukî değerlendirmeyi kim yapacaktır? Bu değerlendirmeyi artık adlî bilişim uzmanı değil, kolluk yapacaktır. adlî bilişim uzman(lar)ının inceleme aşamasından geçmiş verilerden hangilerinin delil olabileceği, o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilir ve adlî makamlara sunulur.
Sunulan raporda ayrıntılı olarak dijital delillerin nasıl elde edildiğinn ilişkin teknik boyutu ve adlî bilişimin hangi metodlarının kullanıldığı da anlaşılır bir dille belirtilir. Hazırlanan raporda ayrıca, olayla ilgili bilgiler, araştırmanın yapıldığı zaman dilimi, incelenen elektronik deliller, inceleme esnasında kullanılan yazılım ve donanımlar hakkında bilgiler, inceleme sırasında kullanılan metodlar, araştırma sonunda ele geçen bulgulara ilişkin bilgilerin yer alması gerekir.

4.11. İade ve Müsadere

Bilgisayardaki verilerin mevcut hâli ile yedeği alınmalı, bilgisayar iade edilmeli ve yapılacak arama işlemi bu yedek üzerinde yapılmalıdır. Şifreli cihazlarda şifre çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar gecikme olmaksızın iade edilir. Yasada düzenlenmemekle birlikte, uygulayıcıların uygulamaları ile bizzat bulundurulması suç olan kredi kartı şifreleri, çocuk pornografisi vb. yedekler verilmemektedir.

Çıkartılacak yedekten şüpheliye veya vekiline örnek verilmesi bu kişilerin isteğine bırakılmıştır. Ancak şüpheliye örnek isteyip istemediği sorulup bu husus kayıt altına alınmalıdır.

5 İNTERNET SÜJELERİNİN SORUMLULUK VE YÜKÜMLÜLÜKLERİ

5. İNTERNET SÜJELERİNİN SORUMLULUK VE YÜKÜMLÜLÜKLERİ, ERİŞİMİN ENGELLENMESİ VE HUKUKA AYKIRI İÇERİĞİN YAYINDAN ÇIKARILMASI (5651 SAYILI YASA)

5.1. İnternet Sujelerinin Sorumluluk ve Yükümlülükleri

5.1.1. İnternet Sujelerinin Bilgilendirme Yükümlülüğü

Bilgilendirme yükümlülüğü 23/05/2007 tarihli ve 26530 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* 3.madesinde düzenlenmiştir.Ticari veya ekonomik amaçlı içerik sağlayıcılar, yer sağlayıcıları ve erişim sağlayıcılar, tanıtıcı bilgilerini, kendilerine ait internet ortamında, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve iletişim başlığı altında, doğru, eksiksiz ve güncel olarak bulundurmakla yükümlüdür. Belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkanlık tarafından ikibin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar idari para cezası verilir.[1]

Yeni düzenleme ile ilgili maddeye 3. fıkra eklenmiş ve *"Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir."* şeklinde bir hüküm getirilmiştir. Bu madde ile bilgilendirme yükümlülüğü açısından TİB'e bir kolaylık sağlanmış ve içerik,yer ve erişim sağlayıcılara madde metninde belirtilen yollar ile bildirim yapılabileceği hükme bağlanmıştır. Bu noktada, ilgili kişinin bildirimden haberdar olup olmadığı konusu gündeme gelecektir. Nitekim bildirimin muhatabına yapılmasının amacı, muhatabın bildiriden haberdar edilerek aksiyon almasını sağlamaktır. Bildirimin doğru bir şekilde muhatabına ulaşmaması hak kaybına neden olmasına yol açabilecektir. Dolayısıyla özellikle *"ve benzeri kaynaklardan"* ile *"diğer iletişim araçları"* şeklindeki ibarelerin açık olması ve bu şekilde ilgililerin hangi yollardan kendilerine bildirim yapılacağını bilmeleri gerekmektedir.

5.1.2. İnternet Süjelerinin Diğer Sorumluluk ve Yükümlülükleri

5.1.2.1. İçerik Sağlayıcılar ve Yükümlülükleri

İçerik sağlayıcı, 5651 sayılı Yasanın 2. maddesinin 1. fıkrasının (f) bendinde, internetortamında kullanıcılara her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler olarak tanımlanmıştır.

Yasanın 4. maddesinde ise, *"İçerik sağlayıcı, internetortamında kullanıma sunduğu her türlü içerikten sorumludur."* denilmek suretiyle içerik sağlayıcıların, internet ortamında kullanıma sundukları, web sitelerine yükledikleri, sanal ortamda yer almasını bir şekilde sağladıkları her türlü içerikten sorumlu oldukları belirtilmektedir. Aynı düzenleme, Uygulama Yönetmeliğinin 6. maddesinde de yer almaktadır.

Yasanın 4. maddesinin 2. fıkrasının ilk tümcesinde *"İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir."* denilmek suretiyle açık bir şekilde içerik sağlayıcıların, bağlantı verdiği ve ulaşılmasını sağladığı başkasına ait içerikten sorumlu olmayacakları kabul edilmektedir.

1 Dülger, s.717.

Yasanın 4. maddesinin 2. maddesinin 2. tümcesinde ise *"Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur."* denilmek suretiyle içerik sağlayıcıların bağlantı sağladıkları içerikten hangi hâlde sorumlu olacakları düzenlenmiştir. Bu düzenlemeyle ne kastedildiği açık değildir. Uygulama Yönetmeliğinin 6. maddesinin 2. fıkrasının 2. tümcesinde de birebir aynı ifade kullanıldığı için yönetmelik uygulamaya da yol göstermemektedir. Öncelikle *"genel hükümlerle"* ifade edilmek istenen nedir? Bu yasanın genel hükümleriyle, Ceza Yasası'nın genel hükümleri mi yoksa Borçlar Yasası'nın genel hükümleri mi kastedilmektedir? Bir içerik sağlayıcı, örneğin kendi web sitesinde açık bir biçimde bir diğer sitenin içeriğinde yer alan belli bir içeriği benimsediğini söylemedikçe, *"benimseme ve ulaşmayı amaçlama"* hangi ölçütlere göre belirlenecek ve nasıl ispat edilecektir? Bir içerik sağlayıcının web sitesi üzerinden içeriğinde çok sayıda eleştirel yazı bulunan bir web sitesine bağlantı vermesi ve bu web sitesini açıkça övmesi ancak bu sitede yer alan bir yazıda belli bazı kişilere hakaretedilmesi hâlinde, bağlantı sağlayan içerik sağlayıcı bu yazıdan dolayı sorumlu olacak mıdır? Bu konuda karşılaşılacak bir başka önemli örnek de aramamotorları ile ilgilidir. İçerik sağlayıcının ücret ödeyerek kendi bağlantısının üst sıralarda görülmesini sağlaması ancak içeriğin hukuka aykırı olması halinde, sözleşmesi gereği bu bağlantıya ulaşılmasını amaçlayan arama motoru bundan sorumlu olacak mıdır?

Bir başka güncel ve önemli örnek ise web 2.0teknolojisinin kullanıldığı web siteleridir. Bu sitelerin kullandığı teknoloji içeriğin, internet ortamında çok hızlı şekilde yayılmasını olanaklı kılmaktadır. Özellikle RSS abonelik sistemlerinin kullanılmasıyla içerik otomatik olarak güncellenebilmekte ve böylelikle bir içeriğin aynı anda binlerce web sitesinde yayınlanması gerçekleşmektedir. Bu şekilde yayılan bir içeriğin suç unsuru içermesi durumunda her bir web sitesinin ayrı ayrı değerlendirilmesi ve içerik sağlayıcının sunuş biçimi değerlendirilerek sorumluluğun belirlenmesi gerekecektir. Web 2.0 teknolojinin son derece yaygın kullanımı dikkate alındığında, bazı durumlarda bir içerikten dolayı binlerce kişinin suça iştirakten sorumlu tutulması söz konusu olabilecektir. Bu durumda eşitlik ilkesi gereğince ya tüm içerik sağlayıcıların sorumluluğuna gidilecek ya da suçta ve cezada şahsilik ilkesi gereğince sadece içeriği oluşturan veya bağlantının sahibi olan kişinin sorumluluğuna gidilmekle yetinilmesi gerekecektir.

Bu listeyi uzatmak mümkündür. Görünen odur ki, yasanın bu maddesi yukarıda aktarılan ve gerçekleşmesi kuvvetle muhtemel olan bu varsayımlar düşünülmeden kaleme alınmıştır. Bunun cezasını ise internetözneleri ve hukukçular çekecektir. Dolayısıyla bu madde, söz konusu varsayımlar ve benzerleri geniş boyutlu düşünülerek yeniden düzenlenmelidir.[2]

Yeni düzenleme ile birlikte maddeye 3. fıkra eklenerek, *"İçerik sağlayıcı, Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında; talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim eder ve Başkanlıkça bildirilen tedbirleri alır."* şeklinde bir düzenleme getirilmiştir. Yeni düzenleme ile TİB'e getirilen bu yetkilere bir çerçeve belirlenmemiş ve istenilecek bilgilerin içeriğinin neler olduğu belirtilmemiştir. Dolayısıyla TİB'e bilginin niteliğinde herhangi bir sınırlama yapılmaksızın geniş bir yetki verilmiştir. Mahkemeler dışındaki bir otoriteye bu kadar geniş yetkiler tanınması, Anayasa ile güvence altına alınmış olan özel hayatın gizliliği

2 Dülger, s.772.

ve haberleşme özgürlüğünü ihlal ettiği gibi, 2010 yılındaki değişiklik ile Anayasa'nın 20. maddesinde güvence altına alınmış olan kişisel verilerin korunması ilkesine aykırılık oluşturmaktadır. AİHS'nin 8. maddesinde düzenlenen kişisel verilerin korunmasına ilişkin düzenlemeye ve henüz yasalaşmamış olsa da AB Veri Koruma Direktifi'ne (95/46 sayılı) uyum çerçevesinde hazırlanan Kişisel Verilerin Korunması Kanun Tasarı'sına da aykırıbir düzenlemedir. Yasa her ne kadar TİB tarafından edinilecek bilgileri trafik bilgisi ile sınırlandırmış olsa da, kullanıcıların trafik bilgilerini takip ederek kimlikleri hakkında çıkarımlarda bulunulması mümkündür, bu da verilerin kişisel veri olduğunu gösterir. Kişisel verilerin korunmasının en temel ilkelerinden biri, verilerin belirli, açık ve meşru amaçlar için işlenmesi bir diğeri ise işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesidir. Dolayısıyla veri depolama yasağı vardır. Ancak getirilen düzenleme ile verilerin hiçbir ölçüt olmaksızın toplanılması öngörülmüştür.

Bununla birlikte, TİB'in mevzuattaki yasal zeminini, Polis Vazife ve Salahiyetleri Kanunu'nun (PVSK) ek 7. maddesidir. İlgili düzenleme polisin istihbarat toplama yetkisini düzenlemektedir ve TİB, telekomünikasyon yoluyla yapılacak iletişimin istihbari veya ceza yargılaması kapsamında tespitini sağlamak amacıyla kurulmuştur.[3] İlgili düzenleme ile TİB'e talebinin yasaya uygunluğunun denetimi yapılmadan ve herhangi bir hâkim kararı olmadan hertürlü bilgiyi toplama yetkisi verilmiştir.

AİHM'ye göre temel hakları etkileyebilecek konularda idari mercilere/ uygulayıcılara aşırı yetki/güç verilmesi, demokrasinin temel kavramlarından olan hukuk devleti ilkesine aykırıdır.[4] Bu çerçevede yasalar açık olarak kullanılacak takdir yetkisinin sınırlarını ve ne şekilde kullanılacağını göstermelidir. Yukarıdaki açıklamalar ile TİB başkanı olarak bir MİT mensubunun atanmış olması birlikte değerlendirildiğinde durum endişe vericidir.

5.1.2.2. Yer Sağlayıcılar ve Yükümlülükleri

Yer sağlayıcılar, 5651 sayılı Yasanın 2. maddesinin 1. fıkrasının (m) bendinde, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler olarak tanımlanmıştır. Türkiye'de yer sağlayıcı olarak faaliyette bulunabilmek için Faaliyet Yönetmeliği'nde belirtilen esaslara göre faaliyet belgesinin alınması gerekmektedir. Söz konusu yer sağlayıcıların kimler olduğu ve faaliyet belgelerine ilişkin ayrıntılı bilgilere BTK'nın web sayfasından ulaşılabilmektedir.

Yasa'nın 5. maddesinde yer sağlayıcının yani bilinen adıyla *"host hizmeti/ bulundurma hizmeti"* verenlerin sorumluluğu *"Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir."* şeklinde düzenlenmiştir. Buna göre yer sağlayıcılar, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildirler. Yasanın gerekçesinde, bu düzenlemenin ASSS ve ATS hükümleri göz önünde bulundurularak hazırlandığı belirtilmiştir. Ayrıca düzenleme bu haliyle AB E – Ticaret Yönergesi'nin 15. maddesiyle de uyumlu bir haldedir.

Bunun yerinde bir düzenleme olduğunu belirtmeliyiz.Aksi yöndeki bir

3 Türkiye Gazeteciler Cemiyeti Raporu, İnternet Ortaminda Yapilan Yayinlarin Düzenlenmesi ve Bu Yayinlar Yoluyla Işlenen Suçlarla Mücadele Edilmesi Hakkinda Kanunda Değişiklik Yapilmasina Dair Kanun Teklifi Raporu, Av. Ersü Oktay Huduti,sf. 7

4 Türkiye Gazeteciler Cemiyeti Raporu, İnternet Ortaminda Yapilan Yayinlarin Düzenlenmesi ve Bu Yayinlar Yoluyla Işlenen Suçlarla Mücadele Edilmesi Hakkinda Kanunda Değişiklik Yapilmasina Dair Kanun Teklifi Raporu, Av. Ersü Oktay Huduti,sf. 8

düzenlemeyle yer sağlayıcıları hizmet verdiği milyonlarca verinin içeriği hakkında bilgi edinmek zorunda bırakmanın ve bundan sorumlu tutmanın hem fiziksel olarak imkânsız hem de son derece adaletsiz olacağı açıktır.

Bu maddenin 2. fıkrasında ise yer sağlayıcıların, yer sağladığı hukuka aykırı içeriği, 5651 sayılı yasanın 8. ve 9. maddelerine göre haberdar edilmesi hâlinde yayından kaldırmakla yükümlü olduğu belirtilmektedir.

Yeni düzenleme ile, maddenin 2. fıkrasındaki *"ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla"* ve *"ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırma"* ibareleri çıkarılarak, Yasa'nın 8. ve 9. maddelerine göre bildirimde bulunulması halinde içeriğin her şartta çıkarılması zorunlu hale getirilmiştir.

5651 sayılı Yasada gerçekleştirilen yeni düzenleme ile, yer sağlayıcılara getirilen bir diğer yükümlülük ise trafik bilgilerinin saklanmasına ilişkindir. Buna göre, yer sağlayıcılar, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikle belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü tutulmuşlardır. Trafik bilgisi 5651 sayılı Yasanın 2. maddesinde internet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerlerin bütünü olarak tanımlanmaktadır.[5] İçerik sağlayıcıların yükümlülüklerini düzenleyen 4. maddenin 3. fıkrası ile getirilen düzenlemeye paralel olarak, ,ilgili maddenin 5. fıkrası ile yer sağlayıcıya, *"Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüğü"* getirilmiştir. Maddenin 6. fıkrası ile, *"Yer sağlayıcılık bildiriminde bulunmayan veya bu Kanundaki yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında Başkanlık tarafından on bin Türk Lirasından yüz bin Türk Lirasına kadar idari para cezası verilir."* şeklinde bir düzenleme getirilmiştir. Madde metninden de anlaşılacağı üzere, TİB'in idari para cezasını tayin için mutlak yetkisi bulunmaktadır.Önceden de ifade ettiğimiz üzere, TİB tarafından talep edilcek bilgiler trafik bilgisi şeklinde sınırlandırılmış olsa da, bilgilerinin incelenmesi neticesinde elde edilecek verilerin her biri kişisel veridir. Nitekim kişilerin internet ortamındaki hareketlerinin incelenmesi neticesinde kolaylıkla kişiler hakkında bilgi dolayısıyla veri elde edilebilir. İlgili fıkra açısından Yasa'nın 4. maddesinin 3. fıkrasına dair değerlendirme, bahsi geçen fıkra için de geçerlidir, bu nedenle tekrar edilmeyecektir. Ancak içerik sağlayıcıdan farklı olarak yer sağlayıcıların yükümlülüklerine uymamaları halinde idari para cezası yaptırımına maruz kalmaları, yer sağlayıcıların bu bilgileri zorunlu olarak paylaşmaları neticesine götürecektir. Bahsi geçen bilgilerin paylaşımına itiraz mekanizması Yasa ile getirilmemekle birlikte, yer sağlayıcıların bilgiyi paylaşmaları konusunda herhangi bir çıkarları olmadığından ve yükümlülüğe uyulmamasının yaptırımı olması nedeniyle bu duruma itiraz etmeyecektir. Bilgisi paylaşılacak kişiler isedurumdan haberdar olmadıklarındanherhangi bir yasal yola başvurma imkânları olmayacaktır, bu durum TİB'in aşırı ölçüde yürütme yetkisiyle donatılmış olduğunu gözler önüne sermektedir.

5.1.2.3. Erişim Sağlayıcılar ve Yükümlülükleri

Erişim sağlayıcılar, 5651 sayılı Yasanın 2. maddesinin 1. fıkrasının (e) bendinde kişilere internet ortamına erişim olanağı sağlayan gerçek veya tüzel kişiler olarak tanımlanmıştır. Türkiye'de erişim sağlayıcı olarak faaliyette bulunabilmek için Faaliyet

5 Dülger, s.724.

Yönetmeliği'nde belirtilen esaslara göre faaliyet belgesinin alınması gerekmektedir. Söz konusu erişim sağlayıcıların kimler olduğu ve faaliyet belgelerine ilişkin ayrıntılı bilgilere BTK'nın web sayfasından ulaşılabilmektedir.

5651 sayılı Yasanın 6. maddesinde erişim sağlayıcıların yani İSS'lerin hukukî sorumluluğu ve yükümlülükleri düzenleme konusu yapılmıştır. Buna göre erişim sağlayıcı öncelikle herhangi bir kullanıcısının yayınladığı hukuka aykırı içeriği, 5651 sayılı Yasa'ya göre haberdar edilmesi hâlinde erişimi engellemekle yükümlüdür. Yeni düzenleme ile madde metninden *"teknik olarak engelleme imkânı bulunduğu ölçüde"* ibaresi çıkarılmıştır. Dolayısıyla, erişim sağlayıcıların engellemeyi gerçekleştirebilmeleri için gerekli her türlü teknik donanım ve yazılıma sahip olmaları gerekemektedir.

Yeni düzenleme ile, ilgili maddenin ilk fıkrasına *"Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla yükümlüdür."* şeklinde bir hüküm eklenmiştir. Madde metninde alternatif yolların neler olduğuna ilişkin herhangi bir açıklama yapılmamıştır. Dolayısıyla erişim sağlayıcıların yükümlülükleri konusunda belirsizlik söz konusudur. Erişim sağlayıcıların tüm yolları araştırma yükümlülükleri bulunmakta mıdır? Eğer böyle bir yükümlülükleri var ise hangi araçlar ile bunu gerçekleştireceklerdir ve bu maliyeti nasıl karşılayacaklardır? Belirtilmiş olunan soruların cevaplandırılmaları önemlidir çünkü yasanın ilgili maddesinin 3. fıkrası ile yükümlülükleri yerine getirmeyen erişim sağlayıcısına Başkanlık tarafından onbin TL'den elli bin TL'ye kadar idari para cezası öngörülmüştür. 5651 sayılı Yasanın 6. maddesinin 1. fıkrasında ikinci olarak erişim sağlayıcının sağladığı hizmetlere ilişkin, ilgili yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü olacakları düzenlenmektedir. Erişim sağlayıcılara iki yıla kadar bütün trafik bilgilerinin saklanmasına yönelik bir yükümlülük getirmek bazı açılardan sakıncalı bazı açılardan ise olumlu bir düzenlemedir. Böyle bir yükümlülük trafik bilgilerinin tutulması için erişim sağlayıcıların ek yatırım yapmasını gerektirecektir. Söz konusu bilgilerin tutulması için ek aygıtlar ve bu aygıtların bulundurulacağı ek tesisler, erişim sağlayıcılar için önemli miktarda maliyet anlamına gelmektedir ki, bu düzenlemenin olumsuz yönüdür. Düzenlemeye diğer yönden bakıldığında ise, bu bilgilerin uzunca bir süre saklanması internet üzerinden işlenen suçlarla mücadele edilmesi açısından çok önemli ve gerekli bilgilerin kaybolmasını önleyecek ve faillerin ortaya çıkarılmasını sağlayacaktır. Bu ise düzenlemenin olumlu yönünü oluşturmaktadır.

İnceleme konusu yasanın 6. maddesinin 1. fıkrasının "c" bedinde ise, erişim sağlayıcının faaliyetine son vermesi durumunda, faaliyetine son vermeden en az üç ay önce durumu Telekomünikasyon Kurumu'na, içerik sağlayıcılarına ve müşterilerine bildirmekle yükümlü olduğu düzenlenmiştir. Fıkranın devamında faaliyetine son verecek erişim sağlayıcının internetiletişimine ilişkin saklamakla yükümlü olduğu trafik bilgilerini bu konuda çıkartılacak yönetmelikte belirtilecek esas ve usullere göre Telekomünikasyon Kurumu'na teslim etmekle yükümlü oldukları belirtilmektedir.

Yeni düzenleme ile 6.maddenin 1. fıkrasının d bendi, *"Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür."* şeklinde düzenlenmiştir.Yine içerik sağlayıcı ve yer sağlayıcının yükümlülüklerinin değerlendirildiği kısımda açıklanmış hususlar aynı şekilde bu bent için de geçerlidir.

5651 sayılı Yasanın 6. maddesinin 2. fıkrasında yukarıda da belirtildiği üzere,

erişim sağlayıcıların kendi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadığını ve hukukî sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü olmadıkları düzenlenmektedir. Bu düzenleme Alman Teleservisler Yasası'nın benzeri olup erişim sağlayıcıların sorumluluğu açısından olumlu bir düzenlemedir.

5651 sayılı Yasa erişim sağlayıcıların sorumluluğunu yer sağlayıcılarla aynı esaslara göre düzenlemiştir. Yasanın 8. maddesinin 10. fıkrasına göre, *"Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adlî para cezası ile cezalandırılır."* 8. maddenin 11. fıkrasında ise, idari tedbir olarak verilen erişim engelleme kararlarının yerine getirilmemesi halinde ise TİB Başkanlığı tarafından erişim sağlayıcısına, on bin TL'den yüz bin TL'ye kadar idari para cezası verileceği düzenlenmektedir. İdarî para cezasının verildiği andan itibaren yirmi dört saat içinde kararın yerine getirilmemesi hâlinde ise, TİB'in yetkilendirmenin iptaline karar verilebileceği düzenlenmektedir.

5651 sayılı Yasanın 6. maddesinin son fıkrasında ise 1. fıkranın (b) ve (c) bentlerinde düzenlenen yükümlülükleri yerine getirmeyen erişim sağlayıcısına Ulaştırma Bakanlığı tarafından on bin TL'den elli bin TL'ye kadar idari para cezası verileceği düzenlenmektedir. Yasanın 8. maddesinin 12 nolu fıkrasında yasada tanımlanan kabahatler dolayısıyla başkanlık veya kurum tarafından verilen idari para cezası kararlarına karşı 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre yasa yollarına başvurulacağı belirtildiği için, 6. maddenin 3. fıkrasına göre idari para cezası verilmesi halinde bu kararın iptali için altmış gün içinde idari yargıda iptal davası açılması mümkündür.[6]

5.1.2.3.1. Erişim Sağlayıcıları Birliği

Yeni düzenleme ile Yasa'ya 6/A maddesi eklenerek erişimin engellenmesi kararlarının uygulanmasının sağlanması için *"Erişim Sağlayıcıları Birliği"* adı altında bir birlik kurulması öngörülmüştür. Madde ile tüm servis sağlayıcıların ve internet erişim hizmeti veren işletmelerin Birliğe üye olması zorunlu kılınmış ve üye olmayan servis sağlayıcıların faaliyette bulunamayacakları dolayısıyla lisanslarının iptal edileceği hükme bağlanmıştır. Bu oldukça ağır bir yaptırımdır. Ayrıca bilindiği üzere, bir işletmeye bağlı lisanslar/ruhsatlar AİHS Protokol No.1'in 1. maddesine göre, mülkiyet hakkı kapsamında korunan bir malvarlığı değeridir. İnternet servis sağlama ruhsatı da bu tip lisanslar arasındadır, dolayısıyla bu tip lisansların hukukî güvenlik ilkesine aykırı olarak iptali mülkiyet hakkının ihlali niteliğindedir.[7] İlgili madde ile 8. madde kapsamı dışındaki tüm erişim engelleme kararlarının erişim sağlayıcılar tarafından yerine getirileceği ve buna dair teknik donanım ve yazılımın erişim sağlayıcılar tarafından edinilmesi zorunlu kılınmıştır. Her ne kadar madde ile Birliğin özel hukuk tüzel kişisi olduğu belirtilmişse de, kuruluşa üyeliğin zorunlu olması ve üye servis sağlayıcıların kar oranlarına göre Birliğe aylık ödeme yapmasının şart koşulması, tüzüğün kendilerince düzenlenememesi ve yürürlüğe girmesi için BTK'nın onayının gerekmesi kısacası özgür irade ile kurulmuş bir kurum olmasası adeta kamu hukuku tüzel kişisi niteliğinde olduğunu göstermektedir.

6 Dülger, s.725.

7 Türkiye Gazeteciler Cemiyeti Raporu, İnternet Ortaminda Yapilan Yayinlarin Düzenlenmesi ve Bu Yayinlar Yoluyla Işlenen Suçlarla Mücadele Edilmesi Hakkinda Kanunda Değişiklik Yapilmasina Dair Kanun Teklifi Raporu, Av. Ersü Oktay Huduti,sf.15

5.1.2.4. Toplu Kullanım Sağlayıcılar ve Yükümlülükleri

Toplu kullanım sağlayıcıları 5651 sayılı Yasanın 2. maddesinde, belli bir yerde ve belli bir sürede internet kullanım olanağı sağlayanlar olarak tanımlanmaktadır. Yasada internet toplu kullanım sağlayıcılar için ticari amaçla hareket edip etmediklerine göre farklı sorumluluk şekilleri öngörülmüştür.

İnternet Toplu Kullanım Sağlayıcıların Yükümlülükleri Yasanın 7. maddesinde "toplu kullanım sağlayıcıların yükümlülükleri" başlığı altında kamuya açık alanlarda ücretsiz olarak ya da "internet kafe" olarak nitelendirilen ticari amaçlı internete erişim sağlayanların hukukî sorumlulukları düzenlenmiştir. Buna göre, ticari amaçla toplu kullanım sağlayıcılar bu faaliyetleri gerçekleştirebilmek için bulundukları yer mülki amirinden izin belgesi almakla yükümlüdürler. Söz konusu izin başvurusu yapıldıktan itibaren otuz gün içerisinde izne ilişkin bilgiler başvurunun yapıldığı yerel mülki amir tarafından Telekomünikasyon Kurumuna (günümüzde BTK'ya) bildirilecektir. İzin belgesi için gerekli bilgilerin doğruluğu ve bu kapsamda ticari amaçlı toplu kullanım sağlayıcıların denetimi yerel mülki amirler tarafından yapılacaktır. İzin belgesinin verilmesine ve denetimine ilişkin esas ve usuller ise ilgili yönetmelikte düzenleme konusu yapılacaktır. Buna göre söz konusu maddeyle internet kafelerin açılması ve faaliyetlerine devamı için izin alınması ve mülki amirin denetimi yöntemi getirilmiştir.

Bu fıkranın tersinden çıkan anlam, ticari amaçlı olmayan toplu kullanım sağlayıcılar için izin ve denetim yönteminin geçerli olmadığıdır. Buna göre üniversiteler, oteller, havaalanları, kütüphaneler gibi yerlerde ticari amaçlı olmayan interneterişim hizmeti verilmesi hâlinde bunun için izin alınması gerekmemekte bu gibi yerlerde internete erişim açısından yerel mülki amirin denetim görevi bulunmamaktadır.

Maddenin 2. fıkrasında ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcıların konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlü olduğu hükme bağlanmıştır. 7. maddenin 4. fıkrasında *"Yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amir yetkilidir."* şeklinde bir düzenleme getirilerektoplu kullanım sağlayıcılarının yükümlülüklerini yerine getirmedikleri durumlarda yaptırım uygulanacağı öngörülmüştür. Aslında toplu erişim sağlayıcıların müşterilerini kasten konusu suç oluşturan içeriklere yönlendirmesi suça iştirak kapsamında TCK'daki genel hükümlere göre değerlendirilecektir, ayrıca bu yasayla da failin kusuruna ilişkin bir belirleme yapılmaksızın benzer bir düzenlemenin yapılması uygun değildir. Bu nedenle söz konusu fıkra 5651 sayılı Yasa'da yer alması gerekmeyen bir düzenlemedir.

5651 sayılı Yasa'nın 8. maddesinin 12 nolu fıkrasında yasada tanımlanan kabahatler dolayısıyla başkanlık veya kurum tarafından verilen idari para cezalarına ilişkin kararlara karşı 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre yasa yollarına başvurulacağı belirtildiği için, 7. maddenin 4. fıkrasına göre idari para cezası verilmesi hâlinde bu kararın iptali için altmış gün içinde idari yargıda iptal davası açılması mümkündür.

İlgli maddenin 3. fıkrası ile, ticari amaçla toplu kullanım sağlayıcılara, ailenin

ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri alma yükümlülüğü getirilmiştir.

Günümüzde gelinen aşama itibariyle hemen hemen herkes toplu kullanım sağlayıcı hâline gelmiştir. İki kişinin çalıştığı ofiste, dört kişinin yaşadığı evde, binden fazla kullanıcının olduğu üniversitede ya da kullanıcı sayısının binlerle ifade edilebileceği havaalanı gibi tesislerin hemen tamamında internete erişim sağlanmakta ve bunu sağlayanlar da 5651 sayılı Yasa'nın düzenlemesine göre toplu kullanım sağlayıcı sıfatını alıp, 7. maddedeki yükümlülüklere tabi olmaktadırlar. Büyük şirketler ya da üniversite gibi kurumlar tarafından bir an için filtreleme yazılımlarının kullanımının özellikle maddî açıdan etkili olacağı kabul edilse dahi evlerde ya da küçük ofislerde ya da işyerlerinde bunun nasıl uygulanacağı veya bu maddî külfetin altından nasıl kalkabilecekleri bir soru işaretidir.

Öte yandan toplu kullanım sağlayıcıların en temel yükümlülüklerinin suç oluşturan içerikler için erişimi önleyici tedbirlerin alınması olduğu, bu yükümlülük bakımından toplu kullanım sağlayıcısının faaliyetlerini ticari amaçla yapıp yapmamasının bir öneminin bulunmadığı ifade edilmektedir. Yasanın gerekçesinde de Avrupa Konseyi'nin 1999/246 ve 2005/854 sayılı Kararları ile üye ülkeleri internetin güvenli kullanılmasının sağlanması için filtreleme ve bloke etme programları geliştirmeye ve aynı amaçla eğitim ve tanıtım faaliyetlerini yaygınlaştırmaya davet ettiği, internet kafeler gibi toplu kullanım sağlayıcıların çocuklar dâhil toplumun her kesimi tarafından internete erişim için yoğun olarak kullanıldığı, bu sebeple söz konusu yerler nezdinde alınacak önleyici tedbirlerin internet ortamında suçla mücadele alanında önemli bir yer tuttuğu ifade edilmektedir. Ancak, yasanın gerekçesinde toplu internet sağlayıcıları yalnızca internet kafelerden ibaretmiş gibi açıklansa da yukarıda ayrıntılı olarak belirttiğimiz üzere yalnızca bunlardan ibaret değildir ve bu açıdan düzenleme hatalı olmuştur.

Toplu Kullanım Yönetmeliği'nde toplu kullanım sağlayıcıların uymaları gereken usul ve esaslar ayrıntılı bir şekilde düzenlenmiştir. Yönetmeliğin 5. maddesi gereğince, erişim sağlayıcılar gibi internettoplu kullanım sağlayıcılar da trafik bilgilerini bir yıl saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü tutulmuşlardır. Ancak yönetmelikte bu yükümlülüğe aykırı davranılmasının yaptırımı yer almamaktadır.[8]

5.1.3. İçeriğin Yayından Çıkarılması Yükümlülüğü

Yeni düzenlemeyle içeriğin yayından çıkartılmasına ilişkin 9. maddesine göre; *"İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir."* Dolayısıyla birinci fıkra ile uyar-kaldır yönteminin kullanılabileceği gibi, kişilik haklarına saldırı olduğunu iddia eden kişiye ikinci bir seçenek olarak doğrudan mahkemeye başvurma hakkı da tanınmıştır. İkinci fıkra ile internet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin taleplerinin içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılması gerektiği belirtilmiştir.

Maddenin 4. fıkrası ile URL bazlı erişim engellenmesi düzenlenmiştir.

8 Dülger, s.717.

Yasada URL adresi; *"ilgili içeriğin internette bulunduğu tam internet adresi"* şeklinde tanımlanmıştır. Yeni düzenleme ile, esas olarak URL engellenmesi yöntemi ile erişimin engellenmesi gerektiği belirtilmiştir. Dolayısıyla hâkim, yalnızca kişilik hakkının ihlal edildiği bölüm ile ilgili olarak erişimin engellenmesi kararı verecektir. Madde metnine göre, ancak URL adresinin engellenmesi ile ihlalin engellenemeyeceği durumlarda tüm yayına yönelik olarak erişimin engellenmesi kararı verilebilecektir. URL adresi ile sınırlı olarak erişimin engellenmesiAnayasa ile korunan temel hak ve özgürlüklere müdahale açısından çok daha doğru bir düzenleme olmuştur.Maddenin 5. fıkrası ile hâkimin erişimin engellenmesi kararını doğrudan Birliğe göndereceği belirtilmiştir. Bu fıkra, 6/A maddesinin 7. fıkrası ile düzenlenmiş olunan, Birliğe yapılan tebligatın erişim sağlayıcılara da yapıldığının kabul edilmesinin bir sonucudur.

Madde ile hâkimin başvuruları en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlayacağı belirtilmiştir.Hâkimin dosya üzerinden değerlendirme yapması ile ilgili kişinin beyanları alınmaksızın karar verilmiş olunacağından kişinin hakkı güvencelerden uzak bir şekilde kısıtlanmış olacaktır.Maddenin beşinci fıkrası ile erişimin engellenmesi kararlarının doğrudan Birliğe gönderileceği belirtilmiştir. Maddeye göre, Birliğe gönderilen erişim engelleme kararı derhal erişim sağlayıcıya gönderilir ve en geç dört saat içinde erişim sağlayıcı tarafından engelleme kararı yerine getirilir. İlgili maddenin 9. fıkrası ile, hâkimin vermiş olduğu erişim engelleme kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi halinde mevcut kararın bu adresler için de uygulanacağı hükme bağlanmıştır.Maddenin altıncı fıkrası ile, TİB'e 5271 sayılı CMK hükümlerine göre itiraz hakkı düzenlenmiştir. Belirtilmiş olunan yükümlülüklerin ihlali halinde, beşyüz günden üç bin güne kadar adlî para cezası öngörülmüştür.

Dokuzuncu madde düzenlemesi, yalnızca hukuka aykırılığa konu içeriğin çıkartılmasını amaçlaması itibariyle ölçülülük ilkesine uygun bir düzenleme olmakla birlikte, kararın muhatabı olan içerik ve yer sağlayıcıların çoğunlukla yurt dışı kaynaklı olması, bu kişilere ait internet açık kaynak irtibat bilgilerinin büyük oranda eksik ve yanlış olması nedeniyle içeriğin yayından çıkartılması kararlarının infazında güçlük çekilmektedir. Söz konusu kararlarda alan adı ve IP den erişimin engellenmesi kararlarında uygulanan merkezi sistem işletilememekte, bu kararların infazı ancak içerik veya yer sağlayıcıyla doğrudan irtibat kurulmasını mecbur kılmaktadır.

Sonuç olarak

Söz konusu zorlukların aşılması sürecinde ulusal ve uluslararası kurum ve kuruluşlarla, internet süjeleriyle, klasik usuller dışında iş birliği süreçlerinin geliştirilmesi büyük önem arz etmektedir. Özellikle yurt dışı kaynaklı internet süjelerinin yurt içi irtibatlarıyla karar mercilerinin doğrudan irtibat kurulması büyük önem arz etmektedir.

Yurt içi irtibatı olmayanlarla mevcut klasik usuller (ki bunların geliştirilmesine, güncellenmesine ihtiyaç bulunmaktadır) ve internetin dağıtık ve dinamik yapısının zorunlu kıldığı yeni iş birliği modelleri (Brezilya Federal savcılık ofisi ile Brezilya Google arasında yapılan özel anlaşma benzeri) geliştirilmesi bir zorunluluktur.

Ayrıca siber suçlar sözleşmesi gibi mevcut uluslararası sözleşmelere dâhil olunarak bu sözleşmeler çerçevesinde oluşturulmuş olan uluslararası mekanizmalardan istifade edilmesi de yine bir mecburiyettir.

Muhatapların irtibat bilgilerinin tespitinde Başkanlık tarafından sunulmakta olan **http://internet.tib.gov.tr** isimli İnternet adresindeki sorgu sonuçlarından faydalanılabilecektir. Bu sayfada açık kaynaklardan elde edilen yurt dışı kaynaklı muhatapların irtibat bilgilerine de yer verilmektedir. Yine Başkanlığın çevrim dışı hizmetlerinden olan **http://tib.gov.tr** adresinde, yurt içi kaynaklı yer sağlayıcıların güvenilir iletişim bilgileri yer almaktadır.

5.1.3.1. Özel Hayatın Gizliliği Nedeniyle İçeriğe Erişimin Engellenmesi

Yeni düzenleme ile en çok tartışılan madde Yasa'nın 9/A maddesinde düzenlenmiştir. İlgili maddenin ilk fıkrasına göre, *"İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Başkanlığa doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir."* Üçüncü fıkra ile, TİB'in kendisine gelen bu talebi uygulanmak üzere derhal Birliğe bildireceği ve kararın en geç dört saat içinde yerine getirileceği hükme bağlanmıştır. Dolayısıyla özel hayatın gizliliği ihlali iddiasında, Anayasa ile korunan başka bir temel hak ve özgürlüğün bu haktan üstün olup olmadığının değerlendirmesi yapılmadan erişimin engellenmesi tedbiri uygulanmış olacaktır. Her ne kadar maddenin 5. fıkrası ile TİB'e talepte bulunan ve hakkının ihlal edildiğini iddia eden kişinin talebini 24 saat içinde sulh ceza mahkemesine sunması gerektiği ve hâkimin en geç 48 saat içinde kararını açıklaması gerektiği belirtilmiş olunsa da, hukuka aykırı bir netice oluşacaktır. Hâkim, özel hayatın gizliliğinin ihlal edilmediği kanaatine vardığında, TİB, tedbiri uygulamış olduğu için hakka müdahale edilmiş olunacaktır. Aksi durumda ise Mahkeme dosya üzerinden değerlendirme yapacağından ilgili kişinin beyanları alınmaksızın karar verilmiş olunacak ve kişinin hakkı güvencelerden uzak bir şekilde kısıtlanmış olacaktır.Maddenin altıncı fıkrasında TİB'e 5271 sayılı CMK hükümlerine göre itiraz hakkı düzenlenmiştir. Yer sağlayıcı ve içerik sağlayıcıya böyle bir itiraz yolu yasa ile düzenlenmemiş olsa da CMK madde 268 çerçevesinde itirazın mümkün olduğunun kabulü gerekmektedir.Ancak bu noktada hâkimin gerekçeli kararı tebliğ edilmeyeceğinden karar metnini görmeden itiraz etmek durumunda kalınacaktır.

Maddenin 8. fıkrası ise gecikmesinde sakınca bulunan hâllerde TİB'e doğrudan erişimin engellenmesi emir verme yetkisi düzenlenmiştir. İlgili fıkranın en büyük sorunu, TİB tarafından verilen kararın yargı denetiminden muaf tutulmuş olunmasıdır. Fıkrada TİB'in vermiş olduğu karara karşı Sulh Ceza Mahkemesi'nde itiraz edilebileceği belirtilmiş olunsa da itiraz edilmediği takdirde herhangi bir mahkeme kararı olmaksızın erişim engellenmesi kararının idari bir otorite tarafından verilebileceği sonucu ortaya çıkmaktadır. Bu fıkra, TİB'in aşırı derecede geniş yetkilerle donatıldığını göstermektedir.

Sonuç olarak, erişim engellenmesi kararlarının mutlaka hâkim kararı ile gerçekleştirilmeleri gerekmektedir. Kişilerin haklarına doğrudan saldırı niteliği taşıyacak olan suçlar ile baş edebilmek ve hızlı bir prosedür sağlanması için yalnızca bu konuda görev yapacak olan ve başvuruların değerlendirilmesi neticesinde erişimin engellenmesi kararı verecek olan ihtisas mahkemeleri kurularak istenilen amaca ulaşılabilir.

5.1.3.2. 5651 sayılı Yasanın 9. maddesi

MADDE 9:

(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir.

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adlî para cezası ile cezalandırılır.

5.1.3.3. Özel Hayatın Gizliliği Nedeniyle İçeriğe Erişimin Engellenmesi

Madde 9/A:

(1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Başkanlığa doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir.

(2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

(3) Başkanlık, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir.

(4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

(5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Başkanlığa gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar.

(6) Hâkim tarafından verilen bu karara karşı Başkanlık tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Başkanlık tarafından yapılır. Bu karara karşı sulh ceza mahkemesine itiraz edilebilir.

5.1.3.3. TürkTicaretKanunun 58/4. Maddesi

III - Basın, yayın, iletişim ve bilişim kuruluşlarının sorumluluğu

MADDE 58:

(1) Haksız rekabet, her türlü basın, yayın, iletişim ve bilişim işletmeleriyle, ileride gerçekleşecek teknik gelişmeler sonucunda faaliyete geçecek kuruluşlar aracılığıyla işlenmişse, 56'ncı maddenin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı davalar, ancak, basında yayımlanan şeyin, programın; ekranda, bilişim aracında veya benzeri ortamlarda görüntülenenin; ses olarak yayımlananın veya herhangi bir şekilde iletilenin sahipleri ile ilan veren kişiler aleyhine açılabilir ancak;

a) Yazılı basında yayımlanan şey, program, içerik, görüntü, ses veya ileti, bunların sahiplerinin veya ilan verenin haberi olmaksızın ya da onayına aykırı olarak yayımlanmışsa,

b) Yazılı basında yayımlanan şeyin, programın, görüntünün, ses veya iletinin sahibinin veya ilan verenin kim olduğunun bildirilmesinden kaçınılırsa,

c) Başka sebepler dolayısıyla yazılı basında yayımlanan şeyin, programın, görüntünün, sesin, iletinin sahibinin veya ilan verenin meydana çıkarılması veya bunlara karşı bir Türk mahkemesinde dava açılması mümkün olmazsa,

yukarıda anılan davalar, yazı işleri müdürü, genel yayın yönetmeni, program yapımcısı, görüntüyü, sesi, iletiyi, yayın, iletişim ve bilişim aracına koyan veya koyduran kişi ve ilan servisi şefi; bunlar gösterilemiyorsa, işletme veya kuruluş sahibi aleyhine açılabilir.

(2) Birinci fıkrada öngörülen hâller dışında, aynı fıkrada sayılan kişilerden birinin kusuru hâlinde sıraya bakılmaksızın dava açılabilir.

(3) 56'ncı maddenin birinci fıkrasının (d) ve (e) bentlerinde yazılı davalarda Türk Borçlar Kanunu hükümleri uygulanır.

(4) Haksız rekabet fiilinin iletimini başlatmamış, iletimin alıcısını veya fiili

oluşturan içeriği seçmemiş veya fiili gerçekleştirecek şekilde değiştirmemişse, bu maddenin birinci fıkrasındaki davalar hizmet sağlayıcısı aleyhine açılamaz, tedbir kararı verilemez. Mahkeme haksız rekabet eyleminin olumsuz sonuçlarının kapsamlı veya vereceği zararın büyük olacağı durumlarda ilgili hizmet sağlayıcısını da dinleyerek haksız rekabet fiilinin sona erdirilmesini veya önlenmesine ilişkin tedbir kararını hizmet sağlayıcı aleyhine de verebilir veya içeriğin geçici olarak kaldırılması dâhil somut olaya uyan uygulanabilir başka tedbirler alabilir.

5.1.3.4. Diğer Kanunlara Göre İçerik Çıkarma

(MK 24,25 ile HMK 399' a göre içeriğin yayından çıkarılması kararı verilebilmektedir.)

Erişimin engellenmesi bölümünde detaylarına yer verilen yasal düzenlemeler kapsamında alınmakta olan erişimin engellenmesi tedbiri kararları, içeriğin yayından çıkartılması şeklinde de alınabilmektedir. 5651 sayılı Yasanın 9. Maddesi kapsamında yaşanılmakta olan kararların infazı, yerine getirilmesi sorunu bu tür kararlar içinde geçerli olabilmektedir.

5.1.4. Filtreleme ve Benzeri Tedbirleri Alma Yükümlülüğü

İnternet toplu kullanım sağlayıcıları ve ticari internet amaçlı toplu kullanım sağlayıcıları konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlüdürler. Ticari amaçlı internet toplu kullanım sağlayıcıları bunlara ek olarak mülki idare amirinden izin belgesi almak, Başkanlık tarafından onaylanan içerik filtreleme yazılımını kullanmakla yükümlüdür.

Ticari amaçlı internet toplu kullanım sağlayıcıların denetimi mahalli mülki amirler tarafından yapılmaktadır.

Mahalli mülki amirden izin belgesi almadan ticari amaçla toplu kullanım sağlayıcılığı yapan kişiye mahalli mülki amir tarafından üçbin Yeni Türk Lirasından onbeşbin Yeni Türk Lirasına kadar idari para cezası verilir.

Ticari amaçlı toplu kullanım sağlayıcılarına internet kafeleri, ticari amaçlı olmayan toplu kullanım sağlayıcılarına ise üniversiteler, kamu kurumları, oteller v.b. örnek verilebilir.

5.1.5. Trafik Bilgisi Tutma Yükümlülüğü

Erişim sağlayıcı trafik bilgisi internet ortamında yapılan her türlü erişime ilişkin olarak abonenin kimlik bilgileri adı ve soyadı adresi ve telefon numarası sisteme bağlandığı tarih ve saat bilgisi sistemden çıkış tarih ve saat bilgisi ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri ifade eder.

Yer sağlayıcı trafik internet ortamındaki her türlü yer sağlamaya ilişkin olarak kaynak IP adresi hedef IP adresi bağlantı tarih ve saat bilgisi istenen sayfa adresi (GET POST komut detayları) ve sonuç bilgileri gibi bilgileri ifade eder.

Mevzuata göre trafik bilgisini,erişim sağlayıcılar altı aydan az ve iki yıldan fazla olmamak üzere, yer sağlayıcılar isebir yıldan az iki yıldan fazla olmamak üzere tutmakla yükümlüdür.

5.1.6. Log Bilgisi Tutma Yükümlülüğü

Kendi iç ağlarında dağıtılan IP adres bilgileri, kullanıma başlama ve bitiş tarih ve saatini, bilgisayarların tekil ağ cihaz numarasını (MAC adresi) ifade eder.

Ancak, bilgisayarların internet ortamına çıkarken hangi gerçek IP adresini aldığı ve bu IP adresi ile hangi yayınlara eriştiği bilgisinin tutulması söz konusu değildir.

IP Log İmzalayıcı Program Tutulan İç IP dağıtım loglarının zaman damgası ile saklanması işlevini görmektedir. **http://www.tib.org.tr** adresinden ücretsiz indirilebilmektedir. Bu program ile log dosyası üretilmemekte, mevcut log dosyasını imzalanmaktadır. Tüm bilgisayarlara değil, sadece ana bilgisayara kurulmalıdır. Tutulan logların saklanma süresi 1 yıldır.

5.1.7. 5651 Sayılı Yasa Kapsamında Erişimin Engellenmesi Kararı Verilecek Suçlar

5.1.8. 5237 Sayılı Yasada Yer Alan Katalog Suçlar

"MADDE 8 – (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),
2) Çocukların cinsel istismarı (madde 103, birinci fıkra),
3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
4) Sağlık için tehlikeli madde temini (madde 194),
5) Müstehcenlik (madde 226),
6) Fuhuş (madde 227),
7)Kumar oynanması için yer ve imkân sağlama (madde 228),
suçları."

5.1.8.1. Müstehcenlik

Öncelikle müstehcenlik kavramının içeriğinin zamana ve yere göre değiştiği neyin müstehcen, neyin erotik ve neyin pornografik olduğunun tanımlanmasının son derece zor olduğu ve aradaki sınırların son derece silik olduğu belirtilmelidir. Bilindiği üzere müstehcenin ve pornografinin ne olduğu, devirden devire değiştiği gibi ülkeden ülkeye ve hatta aynı ülke içinde farklı kültür grupları arasında da değişmektedir. Bununla birlikte, sanatsal, tıbbi, bilimsel ya da benzeri bir değeri olan malzemeler, müstehcen olmayan malzemeler şeklinde değerlendirilebilecektir. Bu bağlamda cinsel bir eğitim kılavuzu ya da cinselliğin antropolojik, sosyolojik, tıbbi veya tarihi yönlerini içeren her türlü içerik müstehcenlik kavramının dışında kalmaktadır. Nitekim TCK'nın 266. maddesinde de bilimsel eserler mutlak bir biçimde müstehcenlik suçunun kapsamı dışında bırakılmıştır. Sanatsal ve edebi değeri olan eserlere ise koşullu bir muafiyet tanınmıştır. Yasa, bir sanatsal ve edebi değeri olan eserin 266. maddenin kapsamı dışında tutulabilmesi için her koşulda müstehcen içeriğe sahip ürünlerin üretilmesinde çocukların kullanılmasını yasaklayan hükme uyulmasını ve çocukların bu tür eserlere ulaşmasının engellenmesini zorunlu tutmaktadır.

Öğretide müstehcenlik, erotizm ve pornografi olarak ikiye ayrılmaktadır. Nasılki, müstehcenliğin tanımı son derece muğlak ise erotizm ve pornografinin tanımı da son derece muğlaktır. Erotizm şiddet içermeyen, aşağılayıcı olmayan ve rızaya dayalı cinsel aktivitelerin sözel ya da görsel temsili olarak tanımlanmaktadır. Erotizm, cinsellik içermesine rağmen cinsel uyarımın ön plana geçmediği ve cinsel organların görünmediği içeriktir. Pornografi ise cinsel organların uyarılmış biçimleriyle betimlenmesi ya da gösterilmesi olarak tanımlanmaktadır. Pornografinin temel amacının salt cinsel uyarılmayı sağlamak olduğu ifade edilmektedir.

Burada belirtilmesi gereken bir önemli konu da yetişkinlerin yer aldığı pornografik materyallerin suç oluşturup oluşturmadığı sorunudur. Bugün sosyo-ekonomik açıdan ve buna koşut olarak genellikle düşünce özgürlüğü açısından gelişmiş ülkelerde yetişkin pornografisine ilişkin materyallerin ve bunların dağıtılmasının suç oluşturmadığına yönelik yerleşik bir anlayış bulunmaktadır. Burada belirtilmesi gereken önemli bir husus da, ABD'de pornografi ve müstehcenlik kavramlarının açık bir biçimde Avrupa Siber Suç Sözleşmesinde olduğundan farklı şekilde tanımlanmakta ve kavramlaştırılmakta olduğudur. Buna göre pornografi düşünce özgürlüğünün içinde sayılmaktayken, müstehcenlik bu özgürlüğün dışında kalmakta ve suç olarak tanımlanmaktadır. Bu ülkede yetişkin pornografisi aslında mağdursuz suç olarak görülmektedir. Suç olarak anılmasının nedeni ise, geçmişten gelen ahlâkahlâkî değerlere dayandırılmaktadır. Ancak burada mağdur olması gereken kişiler söz konusu resim ya da filmlerde manken ya da oyuncu olarak yer alan kişilerdir. Bu film ya da resimlerde yer alan manken veya oyuncular ise on sekiz yaşından büyük olmakta, bu çekimleri yapımcılarla imzalamış oldukları sözleşmeler gereğince ücret karşılığı yapmakta ve kandırılmaları ya da zorla bu çekimlere katılmaları söz konusu olmamaktadır. Dolayısıyla da ceza hukuku anlamında bir mağdur bulunmamaktadır. Diğer yandan bu materyalleri tüketenler açısından ise bunlar açıkta satılmadığı gibi ancak 18 yaşın üstünde olan kişiler tarafından satın alınabilmekte ve izlenebilmektedir. Bu nedenle çocukların psikolojik gelişimlerinin bu materyaller tarafından etkilenmesinin önüne geçilmeye çalışılmıştır. Ayrıca bu materyalleri izleyen yetişkin kişilerin mağduriyeti söz konusu değildir. Bu cinsel açıdan olgunluğa erişmiş kişilerin bilinçli bir tercihidir. Bunların üretilmesinin ve tüketilmesinin ahlâken doğru olup olmadığı ceza hukukunun ilgi alanına girmediği gibi devletin yetişkinleri böyle materyallerden korumak gibi bir görevi de bulunmamaktadır. Çünkü laik devlet vatandaşlarının cinsel hayatlarına ve isteklerine bir başka kişinin özgürlüğünü etkilemedikçe karışmaz, bu ancak dinsel kurallarla yönetilen bir rejimde mümkün olabilir. Bu nedenle laik bir devlete sahip olduğu iddiasında bulunan ülkemizde de bu tür eylemler suç olmaktan çıkarılmalı ve buna ilişkin koruma tedbirleri alınmamalıdır. Yoksa yakında mayolu ya da bikinili bayan resimlerinin bulunduğu web siteleri ya da iç çamaşırı veya naylon kadın çorabı/iç çamaşırı tanıtımı ve satışı yapan sitelerin müstehcen olarak kabul edilmesi ve bu maddeye göre koruma tedbiri kapsamında erişimin engellenmesi ve bunların yöneticilerinin cezalandırılması mümkün olabilecektir. Ancak bu açıklamaların tamamı yetişkin pornografisine ilişkindir, çocuk pornografisi veya yetişkinlere ilişkin ürünlerden çocukların korunması kesinlikle bunun dışındadır. Devletler çocukların bundan korunması için uluslararası sözleşmeler gereğince de sorumludurlar ve her türlü önlemi almalıdırlar.[9]

9 Dülger, s.771.

5.1.8.2. Kumar Oynanması İçin Yer ve İmkan Sağlanması:

Kumar oynanması için yer ve imkân sağlanması suçu da bu kapsamda değerlendirilmelidir. Bireyin kumar oynamayı isteyip istememesi kesinlikle bireysel bir tercihtir. Kumar oynamak için cebinde parası olan insanlar komşu ülkelerde bulunan kumarhaneleri doldurmakta ve buralarda büyük bir ekonomik girdi yaratmaktadırlar. Bu ekonomik girdiden pay alabilmek için ülkemizde de hem somut hem de sanal kumar serbest bırakılmalı ancak oynayabilecek kişiler açısından hem yaş hem de gelir düzeyine ilişkin sınırlamalar getirilmelidir. Aksi takdirde sektör hem yeraltına girip bunu yasa dışı olarak yapmakta hem de komşu ülkeler kendi topraklarında bu faaliyeti sürdürmekte ve söz konusu ekonomik girdiyi yönlendirmektedirler.

Ancak somut durum açısından ülkemizde geçerli olan suç politikasına göre bu eylem suç haline getirilmiştir, bu nedenle sanal alanda kumar oynatılması da açık bir biçimde TCK'nın 228. maddesinde düzenlenmelidir. Diğer yandan kumar oynanması eylemi için erişimin engellenmesi koruma tedbiri uygulanabilecek iken buna göre koruduğu hukuksal değer çok daha önemli olan suç tipleri için bu tedbirin uygulanamayacak olması büyük bir çelişki yaratmaktadır.

Açıkçası yasa koyucu tarafından bu yasa düzenlenirken toplumun ve bireyin çıkarları ile suçla korunan hukuksal değerin öneminden çok bazı ahlâkî kaygılar ön plana çıkartılmıştır. Bu da yukarıda açıklandığı üzere birçok açıdan garip bir yasanın yürürlüğe girmesine neden olmuştur.

Ülkemizde kumarhanelerin yasak olmasının doğurduğu boşluğu, online kumarhaneler doldurmaktadır. Çoğunluğu yurt dışında bulunan online kumar siteleri üzerinden futbol, basketbol, at yarışı ve tenis maçları için bahis oynanabildiği gibi, eş zamanlı olarak poker, rulet veya diğer şans oyunlarının da oynanması mümkündür. Kumar oynanması için gereken para vergi ödenmeyerek havale ve kredi kartı gibi yollarla yurt dışındaki online kumar sitelerine aktarılmaktadır. Bazı durumlarda ise aracı kişiler kullanılarak paranın yurt dışındaki hesaplara aktarılması sağlanmaktadır. Bu şekilde internet üzerinden oynanan kumar oyunları hem suç gelirlerinin aklanmasında kullanılmakta hem de vergi kaybı ve kaçağına yol açmaktadır. Türkiye'de 1,5 milyon kişinin internet üzerinden kumar ve bahis oynadığı, online kumar işletmelerinin yıllık cirolarının 1 milyar doları aştığı tahmin edilmektedir. Yazılımların uyumlu hale getirilmesi sayesinde, cep telefonu üzerinden dahi kumar oynamak mümkün hale gelmiştir. Bu nedenle online kumar sitelerinin ziyaretçilerinin hızlı bir şekilde artmakta olduğu belirtilmektedir. Zîra internet üzerinden işletilen kumarhaneler daha çok denetimin az olduğu ve vergi cenneti olarak bilinen yerler üzerinden hizmetlerini sürdürmektedirler. Bu sayede hukuksal sorumluluklardan kurtuldukları gibi vergi ve suç gelirlerinin aklanmasına ilişkin denetimlerden de kurtulmaktadırlar. Ayrıca bu tür kumarhanelerin yatırım ve işletme maliyetleri normal kumarhanelere göre çok düşük olduğu için online kumarhaneler çok daha yüksek oranlarda ikramiye dağıtmakta ve bu durum daha çok tercih edilmelerine neden olmaktadır.

Bu konuda değinmek istediğimiz bir başka husus ise çocukların kumar oynaması için yer ve imkân sağlanmasının TCK'nın 228. maddesinde yer alan suçun nitelikli hâli olarak düzenlenmesidir. 228. maddenin 2. fıkrasında yer alan bu düzenlemenin internetortamında işlenen suçlar açısından uygulanması yönünden bazı engeller bulunmaktadır. Şu an için teknik açıdan web sitelerinin ziyaretçilerinin yaşlarının doğru olarak tespit edilmesi mümkün değildir. Birçok web sitesine girmek

için ana sayfalarında yer verilen yaş doğrulama sistemlerinin kolayca aşılması mümkündür. Dolayısıyla çocukların kumar oynaması için yer ve imkân sağlanıp sağlanmadığının tespiti son derece zordur. Ayrıca bu durum tespit edilse dahi, failin çocukların kumar oynaması içim yer ve imkân sağladığını bilerek eylemini gerçekleştirdiğinin ispat edilmesi gerekir ki, bu eylemin internette gerçekleştirilmesi halinde failin ikrarı dışında bu hususun ispatı mümkün değildir.

5651 sayılı Yasanın yürürlüğe girdiği ilk zamanlarda kumar oynanması için yer ve imkân sağlanması suçuna ilişkin erişimin engellenmesi uygulaması çok fazla olmamasına rağmen, son zamanlarda bu durum değişmiştir. İnternet üzerinden kumar oynatan sitelerde dolaşan para miktarının artması ve bu sitelere yönelik başta Millî Piyango İdaresi olmak üzere kamu otoritelerinin denetimlerini arttırması sonucunda TİB'in bu suça ilişkin engelleme işlemlerinde de artma olduğu görülmektedir.

Son olarak, 7258 sayılı Yasanın 5. maddesinin 2. fıkrasında, bu tür oyunların internet üzerinden oynatılması ihtimali göz önünde bulundurularak internet ortamına ilişkin özel bir düzenleme yapılmıştır. Buna göre, yurt dışında oynatılan her çeşit bahis ve şans oyunlarının internet yoluyla veya başka bir şekilde erişim sağlanarak Türkiye'de oynanmasına olanak sağlanması suç olarak düzenlenmiştir. Buna paralel olarak bahis veya şans oyunlarını oynamaya teşvik edenler hakkında da düzenleme yapılmıştır. İnternet ortamında bahis oynatanlar reklamlarını da internet ortamında yapmaktadırlar. Bu tür sitelerinin yayılmasını önlemek için 7258 sayılı Yasada kişileri her türlü bahis veya şans oyunları oynamaya teşvik etme suç olarak kabul edilmiştir. Bu suçla mücadeleyi daha da etkin hale getirmek için, 7258 sayılı Yasada yer alan suçlarla ilgili olarak 5651 sayılı Yasaya göre erişimin engellenebileceği kabul edilmiştir.[10]

5.1.8.3. Atatürk Aleyhine İşlenen Suçlar

5651 sayılı Yasanın 8. maddesinin 1. fıkrasının (a) bendi uyarınca Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçların internet ortamında yapılan yayınlarla oluştuğu yönünde şüphe bulunması durumunda erişimin engellenmesi kararı verilebilecektir.

5651 sayılı Yasada yer alan erişim engelleme nedenlerine ilişkin en yoğun eleştiri ve tartışmalar Atatürk'e hakaret nedeniyle Youtube video paylaşım sitesine erişim engellendiğinde ortaya çıkmıştır. Dünyanın en çok ziyaret edilen sitelerinden birisi olan Youtube'a erişim 5651 sayılı yasanın yürürlüğe girmesinden önce çeşitli mahkemeler tarafından alınan kararlarla engellenmiştir.

Bu suç bağlamında 5651 sayılı Yasa yürürlüğe girdikten sonraki ilk erişim engelleme kararı Ankara 11. Sulh Ceza Mahkemesi tarafından verilmiştir. Bunun dışında da pek çok mahkeme tarafından benzer gerekçelerle Youtube web sitesine erişimin engellenmesi kararı verilmiştir. Söz konusu kararlar farklı zamanlarda kaldırılmış, ancak söz konusu site uzun süre erişime kapalı tutularak, dünya gündeminde dahi yer almıştır. Bu bağlamda Youtube'a erişimin engellenmesi AB'nin Türkiye hakkında yayınladığı 2008 İlerleme Raporu'nda eleştiri konusu yapılmıştır. Buna rağmen, erişim engellemenin uzun süre kaldırılmamasının esas sebebinin yayıncı şirketin gereken ve beklenen işbirliğini göstermemesi olduğu ifade edilmiştir.[11]

10 Dülger, s.775.

11 Dülger, s.777.

5.1.9. Diğer Yasalarda Erişimin Engellenmesi Kararı Verilebilecek Suçlar

5.1.9.1. FSEK-EK-4 madde

Ek Madde 4 - (Ekmadde: 03/03/2001 - 4630/37. md.)

Eser ve eser sahibi ile eser üzerindeki haklardan herhangi birinin sahibi veya eserin kullanımına ilişkin süreler ve şartlar ile ilgili olarak eser nüshaları üzerinde bulunan veya eserin topluma sunulması sırasında görülen bilgiler ve bu bilgileri temsil eden sayılar veya kodlar yetkisiz olarak ortadan kaldırılamaz veya değiştirilemez. Bilgileri ve bu bilgileri temsil eden sayıları veya kodları yetkisiz olarak değiştirilen veya ortadan kaldırılan eserlerin asılları veya kopyaları dağıtılamaz, dağıtılmak üzere ithal edilemez, yayınlanamaz veya topluma iletilemez.

Yukarıdaki fıkra hükümleri fonogramlar ve fonogramlarda tespit edilmiş icralar bakımından da uygulanır.

(Değişik fıkra:03/03/2004 - 5101/25.mad)*1* Dijital iletim de dahil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla servis ve bilgi içerik sağlayıcılar tarafından eser sahipleri ile bağlantılı hak sahiplerinin bu Kanunda tanınmış haklarının ihlâli halinde, hak sahiplerinin başvuruları üzerine ihlâle konu eserler içerikten çıkarılır. Bunun için hakları haleldar olan gerçek veya tüzel kişi öncelikle bilgi içerik sağlayıcısına başvurarak üç gün içinde ihlâlin durdurulmasını ister. İhlalin devamı hâlinde bu defa, Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlale devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir. İhlâlin durdurulması halinde bilgi içerik sağlayıcısına yeniden servis sağlanır. Servis sağlayıcılar, bilgi içerik sağlayıcılarının isimlerini gösterir listeyi her ayın ilk iş günü Bakanlığa bildirir. Servis sağlayıcılar ile bilgi içerik sağlayıcıları, Bakanlıkça istendiği takdirde her türlü bilgi ve belgeyi vermekle yükümlüdür. Bu maddede belirtilen hususların uygulanmasına ilişkin usul ve esaslar Bakanlık tarafından çıkarılacak bir yönetmelikle belirlenir.

5.1.9.2. 7258 Sayılı Futbol ve Diğer Spor Müsabakalarında Bahis Ve Şans Oyunlarının Düzenlenmesi Hakkındaki Kanunun 5. Maddesi

Madde 5 - (Değişik madde: 22/02/2007-5583 S.K./3.mad;Değişik madde: 23/01/2008-5728 S.K./256.mad)

Kanunun verdiği yetkiye dayalı olmaksızın, spor müsabakaları ile ilişkili olarak sabit ihtimalli veya müşterek bahis oynatanlar, oynanmasına yer veya imkân sağlayanlar, bir yıldan üç yıla kadar hapis ve onbin güne kadar adlî para cezasıyla cezalandırılır.

Yurt dışında oynatılan her çeşit bahis veya şans oyunlarının internet yoluyla ve sair suretle erişim sağlayarak Türkiye'den oynanmasına imkân sağlayan kişiler, iki yıldan beş yıla kadar hapis cezasıyla cezalandırılır.

Her türlü bahis veya şans oyunlarıyla bağlantılı olarak para nakline aracılık eden kişiler, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezasıyla cezalandırılır.

Kişileri, reklam vermek ve sair surette, her türlü bahis veya şans oyunlarını oynamaya teşvik edenler, altı aydan iki yıla kadar hapis ve üçbin güne kadar adlî para cezasıyla cezalandırılır.

Bu maddede tanımlanan suçlarla bağlantılı olarak, her türlü bahis veya şans oyunlarının oynanmasına tahsis edilen veya oynanmasında kullanılan ya da suçun konusunu oluşturan eşya ile bu oyunların oynanması için ortaya konulan veya oynanması suretiyle elde edilen her türlü mal varlığı değeri, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun eşya ve kazanç müsaderesine ilişkin hükümlerine göre müsadere edilir.

Bu maddede tanımlanan suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Bu maddede tanımlanan suçlarla ilgili olarak, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun erişimin engellenmesine ilişkin hükümleri uygulanır.

5.1.9.3. 633 Sayılı Diyanet İşleri Başkanlığı Kuruluş ve Görevleri Hakkındaki Kanun 6. Maddesi

Madde 6 *- (Değişik madde: 26/04/1976 - 1982/1 md.; İptal: Anayasa Mahkemesinin 18/12/1979 tarihli ve E. 1979/25, K. 1979/46 sayılı kararı ile; Değişik madde: 01/07/2010-6002 S.K./5.mad.)*

Mushafları İnceleme ve Kıraat Kurulu, bir başkan ile sekiz üyeden oluşur. Kurul Başkan ve üyelerinin görev süreleri beş yıldır. Süresi sona erenler yeniden atanabilir.

Mushafları İnceleme ve Kıraat Kurulu Başkan ve üyelerinde aşağıdaki nitelikler aranır:

a) Başkanlıkta en az üç yıl görev yapmış olmak.

b) Dini yüksek öğrenim mezunu olmak.

c) Hafız olmak.

d) Aşere, takrib, tayyibe alanında yetkinliği Başkanlıkça kabul edilmiş olmak veya tefsir alanında doktora yapmış olmak.

Mushafları İnceleme ve Kıraat Kurulunun görevleri şunlardır:

a) Mushafların, cüzlerin, mealli mushafların ve Kur'an-ı Kerim metinlerinin hatasız ve eksiksiz basım ve yayımını sağlamak üzere kontrol ettikten sonra mühürlemek veya onaylamak.

b) Hatalı ve noksan olarak basılan veya yayımlanan mushaf ve cüzler ile sesli veya görüntülü Kur'an-ı Kerim yayınlarını tespit etmek.

c) Kıraat ilmi ile ilgili çalışmalar yapmak ve arşiv oluşturmak.

Basımcı ve yayımcılar, basım ve yayımını yaptıkları mushaf ve cüzler ile sesli ve görüntülü Kur'an-ı Kerim yayınlarından imzalı ikişer adedini Başkanlığa gönderir.

Hatalı ve noksan olarak basıldığı veya yayımlandığı Kurul tarafından tespit edilen mushaf ve cüzler ile sesli ve görüntülü Kur'an-ı Kerim yayınları, Başkanlığın

müracaatı üzerine, yayımın yapıldığı yer sulh hukuk mahkemesi kararı ile toplatılır ve imha edilir.

Beşinci fıkra kapsamına giren yayının internet ortamında yapılması halinde, Başkanlığın müracaatı üzerine, sulh hukuk mahkemesi bu yayınla ilgili olarak erişimin engellenmesi kararı verir. Bu kararın bir örneği gereği yapılmak üzere Telekomünikasyon İletişim Başkanlığına gönderilir.

Sulh hukuk mahkemesinin beşinci ve altıncı fıkralar hükümlerine göre verdiği kararlara ve Başkanlığın talebinin reddine dair kararlarına karşı tefhim veya tebliğden itibaren iki hafta içinde asliye hukuk mahkemesinde itiraz yoluna gidilebilir. İtiraz üzerine verilen karar kesindir.

Toplatma ve imha kararına veya erişimin engellenmesi kararına itiraz edilmiş olması, karara konu teşkil eden yayınların toplatılmasına ve erişimin engellenmesine engel teşkil etmez.

Toplatma ve imha kararına konu teşkil eden yayınlar, bu karara süresi içinde itiraz edilmediği veya yapılan itiraz reddedildiği takdirde imha edilir.

5.1.9.4. 556 sayılı Markalar hakkında KHK

27/06/1995 tarihlive 556 sayılı Markaların Korunması Hakkında Kanun Hükmünde Kararname'ye göre ;

Madde 76 *- Bu Kanun Hükmünde Kararnamede öngörülen türde dava açan veya açacak olan kişiler, dava konusu markanın kendi marka haklarına tecavüz teşkil edecek şekilde Türkiye'de kullanılmakta olduğunu veya kullanılması için ciddi ve etkin çalışmalar yapıldığını ispat etmek şartıyla, davanın etkinliğini temin etmek üzere, ihtiyati tedbire karar verilmesini talep edebilir.*

İhtiyati tedbir talebi, dava açılmadan önce ve ya dava ile birlikte veya daha sonra yapılabilir. İhtiyati tedbir talebi, davadan ayrı olarak incelenir.

İhtiyati Tedbirin Niteliği

Madde 77 *– İhtiyati tedbirler, verilecek hükmün etkinliğini tamamen sağlayacak nitelikte olmalı ve özellikle aşağıda belirtilen tedbirleri kapsamalıdır:*

a) Davacının marka hakkına tecavüz teşkil eden fiillerin durdurulması,
b) Marka hakkına tecavüz edilerek üretilen veya ithal edilen şeylere Türkiye sınırları içinde veya gümrük ve serbest liman veya bölge gibi olanlar dahil, bulundukları her yerde el konulması ve bunların saklanması,
c) Herhangibirzararıntazminibakımındanteminatverilmesi.

Hukuk Usulü Muhakemeleri Kanunu Hükümlerinin Uygulanması

Madde 78 *– Tesbit talepleri ve ihtiyati tedbirlerle ilgili diğer hususlarda Hukuk Usulü Muhakemeleri Kanunu hükümleri uygulanır.*

5.1.9.5. HMK'nın 389 uncu maddesi

Madde 399 - (1) Lehine ihtiyati tedbir kararı verilen taraf, ihtiyati tedbir talebinde bulunduğu anda haksız olduğu anlaşılır yahut tedbir kararı kendiliğinden kalkar ya da itiraz üzerine kaldırılır ise haksız ihtiyati tedbir nedeniyle uğranılan zararı tazminle yükümlüdür.

(2) Haksız ihtiyati tedbirden kaynaklanan tazminat davası, esas hakkındaki davanın karara bağlandığı mahkemede açılır.

(3) Tazminat davası açma hakkı, hükmün kesinleşmesinden veya ihtiyati tedbir kararının kalkmasından itibaren, bir yıl geçmesiyle zamanaşımına uğrar.

5.1.9.6. 4733 sayılı Kanunun 8. maddesi

Madde 8 - (Değişik madde: 23/01/2008-5728 S.K./498.mad;Değişik Madde: 03/04/2008-5752 S.K./3.mad)

Ticari amaç olmaksızın, kendi ürettiği ürünleri kullanarak elli kilogramı aşmayan sarmalık kıyılmış tütün elde eden veya üçyüzelli litreyi aşmayan fermente alkollü içki imal edenler haricinde, Kurumdan tesis kurma ve faaliyet izni almadan; tütün işleyenler veya tütün mamulleri, etil alkol, metanol ya da alkollü içki üretmek üzere fabrika, tesis veya imalathane kuran ve işletenler bir yıldan üç yıla kadar hapis ve beşbin günden onbin güne kadar adlî para cezası ile cezalandırılır. Bu Kanunun 6 ncı maddesinin ikinci ve üçüncü fıkralarına aykırı hareket edenler ile tesislerinde izin verilen kategori dışında faaliyette bulunanlara da aynı ceza verilir.

(Mülga fıkra: 28/03/2013-6455 S.K./31. md)
(Mülga fıkra: 28/03/2013-6455 S.K./31. md)
(Mülga fıkra: 28/03/2013-6455 S.K./31. md)

Tütün, tütün mamulleri, etil alkol, metanol ve alkollü içkiler piyasasında mal veya hizmet üreten, işleyen, ihraç veya ithal eden, pazarlayan, alan veya satan gerçek ve tüzel kişilere aşağıda yazılı idari yaptırımlar uygulanır:

a) Bu Kanun veya ilgili mevzuat gereğince Kurum tarafından istenilen ticari faaliyetlerini gösterir satış veya faaliyet raporlarını veya bilgi, belge ve numuneleri yazılı uyarıya rağmen belirlenen süre içinde vermeyenlere, yanlış veya yanıltıcı bilgi veya belge verenlere, gerekli tesis ve yerleri incelemeye açmayanlara ellibin Yeni Türk Lirasından ikiyüzellibin Yeni Türk Lirasına kadar idari para cezası verilir.

b) Üreticiden satın aldıkları tütünleri satış merkezlerine veya Kuruma tescil ettirmeyenlere, yazılı sözleşme yapma tarihine uymayanlara, işleme açılış ve kapanışları ile tütün stoklarını ve tütün depolarını süresi içinde bildirmeyenlere, izinsiz standart dışı işleme yapanlara, bu Kanunda tütün eksperi unvanına sahip olanlar tarafından yapılması öngörülen işleri yetkisiz kişilere yaptıranlara, yazılı sözleşme esası veya açık artırma yöntemi ile yapılan alım satım kapsamındaki yükümlülüklerini süresi içinde yerine getirmeyenlere onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idari para cezası verilir. Bu hüküm Kurumdan izin almadan bir yere mahsus tütün çeşidinin tohum veya fidelerini başka çeşitlere ayrılmış olan yerlere ekenler, dikenler veya bu amaçlarla taşıyanlar hakkında da uygulanır.

c) İzin almadan veya güncelleme yapmadan, ana girdilerde veya ürün ambalajında değişiklik yaparak ürünleri piyasaya arz edenlere ellibin Yeni Türk Lirasından beşyüzbin Yeni Türk Lirasına kadar idari para cezası verilir.

d) Kurumdan izin almaksızın işleme veya üretim tesislerinde proje tadilat kapsamındaki işlemleri yapan, kurulu makinelerini ülke içerisinde kısmen veya tamamen aynı firma tarafından kurulan yeni veya eski bir fabrikaya nakleden, başka bir firmaya devreden ya da ülke dışına çıkaranlara veya bildirimde bulunmaksızın faaliyetini sona erdirenlere ellibin Yeni Türk Lirasından beşyüzbin Yeni Türk Lirasına kadar idari para cezası verilir.

e) Kurumdan izin almadan veya bildirimde bulunmadan dökme alkollü içkileri piyasaya arz eden, sevkiyatını yapan veya izin verilen yerlerden farklı yerlerde depolayanlara ikiyüzbin Yeni Türk Lirası idari para cezası verilir.

f) Kurumdan belge almamış kişilerden ürün alan veya bu kişilere ürün satan ya da belgesinde belirtilen iş yeri dışında satış yapan toptan veya perakende tütün mamulü, etil alkol, metanol veya alkollü içki satıcıları ya da açık içki satıcılarına bin Yeni Türk Lirasından onbin Yeni Türk Lirasına kadar idari para cezası verilir.

g) Kurumdan satış belgesi almadan tütün mamulleri, etil alkol, metanol ve alkollü içkilerin toptan satışını yapanlara ellibin Yeni Türk Lirası; perakende satışını yapanlara ise beşbin Yeni Türk Lirası idari para cezası verilir.

h) Kurumdan yetki belgesi almadan veya bildirimde bulunmadan tütün ticareti yapanlara ellibin Yeni Türk Lirası idari para cezası verilir.

ı) Kurumdan uygunluk belgesi almadan enfiye, çiğneme, nargile tütünü veya yaprak sigara kâğıdı ya da makaron üretenler ile satan veya satışa arz edenlere, (...) beşbin Yeni Türk Lirası idari para cezası verilir.*

j) Yetkili olmadıkları halde, açık olarak içki satışı veya sunumu yapanlar ile satışa sunulan tütün mamulleri, etil alkol, metanol ve alkollü içkileri arz ambalajlarını bozmak veya bunları bölmek suretiyle satanlara bin Yeni Türk Lirasından onbin Yeni Türk Lirasına kadar idari para cezası verilir.

k) Tütün mamulleri veya alkollü içkilerin tüketicilere satışını; (...) internet, televizyon, faks ve telefon gibi elektronik ticaret araçları ya da posta ile sipariş yöntemi kullanarak yapmak üzere satış sistemi kuran veya faaliyette bulunanlara yirmibin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idari para cezası verilir.Satışın internet ortamında yapılması halinde, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda öngörülen usullere göre erişimin engellenmesine karar verilir ve bu karar hakkında da anılan Kanun hükümleri uygulanır.**

1) Tütün mamulleri veya alkollü içkileri satış yerlerindeki raf veya standlara, her türlü teşhir ünitesine, reklam ve tanıtımına ilişkin mevzuata ve Kurum düzenlemelerine aykırılık oluşturacak veya herhangi bir firmaya üstünlük sağlayacak şekilde yerleştirenlere otuzbin Yeni Türk Lirası idari para cezası verilir.

m) Tütün mamulleri veya alkollü içkilerin kullanımını ve satışını özendirici veya teşvik edici kampanya, promosyon, reklam ve tanıtım yapılmasını önlemek amacıyla Kurum tarafından bu Kanun uyarınca yapılan düzenlemelere aykırı hareket edenlere otuzbin Yeni Türk Lirası idari para cezası verilir.

n) Tütün mamulleri veya alkollü içkileri; otomatik satış makinesi ile satanlara veya bahis oynatmak veya ödül vermek gibi yollarla verenlere, fiilleri suç oluşturmadığı takdirde ellibin Yeni Türk Lirasından ikiyüzellibin Yeni Türk Lirasına kadar idari para cezası verilir.

o) (Ek bend: 13/02/2011-6111 S.K 175. mad.) Ticari amaçla sarmalık kıyılmış tütün üretenler ile satan veya satışa arz edenlere ürettikleri, sattıkları veya satışa arz ettikleri tütünün;50 kilograma kadar (50 kilogram dâhil) olması halinde 250 TL.50 kilogramdan 100 kilograma kadar (100 kilogram dâhil) olması halinde 500 TL.100 kilogramdan 250 kilograma kadar (250 kilogram dâhil) olması halinde 1.500

TL.250 kilogramdan 500 kilograma kadar (500 kilogram dâhil) olması halinde 3.000 TL.500 kilogramdan fazla olması halinde 5.000 TLidari para cezası verilir.

Yukarıda sayılan fiiller dışında, bu Kanun ile 4250 sayılı Kanuna veya bu kanunlara göre yürürlüğe konulmuş yönetmeliklere ya da Kurumca verilen belgelerde yer alan şartlara uyulmadığının tespiti halinde, ilgili gerçek ve tüzel kişiler uyarılır ve aykırılığın giderilmesi için uygun bir süre verilir. Her işlem için verilecek süre Kurumca belirlenir. Verilen süre sonunda aykırılığın devam etmesi halinde veya aykırılığın giderilmesinin mümkün olmadığı hallerde süre verilmeksizin Kurumca verilen belgeler iptal edilir.

İdari para cezaları, fiillerin tekrarı halinde, bir önceki cezanın iki katı olarak verilir. Beşinci fıkranın (c) bendinde sayılan fiillerin tekrarı halinde ayrıca ihlale konu ürünün piyasaya arzının bir yıla kadar durdurulmasına; (a), (b), (d), (e), (f), (j), (k), (l), (m) ve (n) bentlerinde sayılan fiillerin, ilk fiilin işlenmesinden sonraki beş yıl içinde üçüncü defa işlenmesi halinde ise belgelerin iptaline karar verilir. Satış belgesi iptal edilen satıcılar, satış belgesi iptaline konu iş yerinde aynı işletme adı altında faaliyette bulunan üçüncü kişiler ile satış belgesi iptal edilen satıcılarca belge iptaline konu iş yerinin farklı işletme adı altında fiilen işletilmesi halinde, bu işletme üzerine kayıtlı görünen üçüncü kişiler adına iki yıl süreyle yeni belge başvurusunda bulunulamaz.

(Değişik fıkra: 13/02/2011-6111 S.K 175. mad.) Bu Kanuna, 4250 sayılı Kanuna veya 5607 sayılı Kanuna aykırı fiillerden dolayı haklarında kesinleşmiş mahkûmiyet kararı olanlara, Kurumun düzenlemekle yükümlü olduğu piyasalarda faaliyete ilişkin hiçbir belge verilmez, verilmiş olanlar Kurumca iptal edilir. Mahkemece verilecek mahkûmiyet kararında, kararın kesinleşmesine kadar faaliyete ilişkin tüm belgelerin askıya alınmasına da karar verilir. Yargılama sonuna kadar üretici ve ithalatçılara yetkili idarece uygun görülecek miktarda bandrol, etiket, hologram, pul, damga veya benzeri işaretler verilebilir. Söz konusu fiillerin kamu sağlığını veya tütün ve alkol piyasasının güvenliğini bozucu nitelikte olması halinde, yargılama sürecinde yetkili mahkemece mevcut delil durumuna göre belgelerin askıya alınmasına tedbiren karar verilir.

Beşinci fıkranın (f), (g), (h), (ı) ve (j) ile (o) bentlerinde yazılı fiiller hakkında idari yaptırım uygulamaya ve bu fiillerin konusunu oluşturan her türlü eşyanın mülkiyetinin kamuya geçirilmesi kararını vermeye mahalli mülki amirler, diğer bentlerde yazılı fiiller hakkında idari para cezası vermeye Kurum yetkilidir. Mahalli mülki amirlerce uygulanan idari yaptırımlar onbeş gün içinde Kuruma iletilir.*

Bu Kanun hükümlerine göre verilen idari yaptırım kararlarına karşı 6/1/1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir. Ancak, idare mahkemesinde dava, işlemin tebliği tarihinden itibaren onbeş gün içinde açılır. İdare mahkemesinde iptal davası açılmış olması, kararın yerine getirilmesini durdurmaz.

İdari yaptırımlara ilişkin olarak bu Kanunda hüküm bulunmayan hallerde 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanunu hükümleri uygulanır.

(Ek fıkra: 28/03/2013-6455 S.K./31. md) Kurum piyasa faaliyetlerine ilişkin olarak tütün, tütün mamulleri, etil alkol, metanol ve alkollü içkiler piyasasında mal veya hizmet üreten, işleyen, ihraç veya ithal eden, pazarlayan, alan veya satan gerçek ve tüzel kişiler ile bunların yetkilileri hakkında açılan kamu davalarını katılan

sıfatıyla takip edebilir. Bu konularla ilgili olarak suç duyurusunda bulunabileceği gibi mevzuatın uygulanması açısından, adlî ve mülki makamlardan yaptırım talebinde bulunabilir.

(Ek fıkra: 28/03/2013-6455 S.K./31. md) Bu Kanuna göre idari para cezalarının veya idari yaptırımların uygulanması, bu Kanunun diğer hükümlerinin ve diğer kanunlarda yer alan ceza ve tedbirlerin uygulanmasına engel teşkil etmez.

(Ek fıkra: 28/03/2013-6455 S.K./31. md) Her türlü uyuşturucu madde, alkollü içki, tütün ve tütün mamulleri bağımlılığı ile mücadele etmek amacıyla Türkiye Yeşilay Cemiyetine 5018 sayılı Kanunun 29 uncu maddesi hükmüne tabi olmaksızın yardım yapılmak üzere, Sağlık Bakanlığı bütçesinde gerekli ödenek öngörülür.

5.2. Koruma Tedbiri Olarak Erişimin Engellenmesi

5.2.1. Yasal Dayanak

Yasanın 8. maddesinin 2. fıkrasında bir ceza muhakemesi koruma tedbiri olarak "erişimin engellenmesi" düzenlenmiştir. Bunun bir ceza muhakemesi koruma tedbiri olduğu 8. maddenin 2. fıkrasında *"koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarih ve 5271 sayılı Ceza Muhakemesi Kanununa göre itiraz edilebilir"*, 10. fıkrada *"koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen..."* ve 11. fıkrada *"idari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi hâlinde..."* düzenlemelerinden anlaşılmaktadır. Yoksa bunun bir koruma tedbiri olduğu başlığında ya da fıkranın içeriğinde belirtilmemektedir. Bu ise yasa yapma tekniği açısından son derece olumsuz bir düzenleme tarzıdır, zîra yasa maddesi adeta bulmaca hâline getirilmiştir.[12]

5.2.2. Kararı Verebilecekler

Erişimin engellenmesi kararı, soruşturma evresinde yargıç, kovuşturma evresinde ise mahkeme tarafından verilecektir. Soruşturma evresinde, gecikmesinde sakınca bulunan hâllerde cumhuriyet savcısı tarafından erişimin engellenmesine karar verilebilecektir. Erişimin engellenmesine cumhuriyet savcısı tarafından karar verilmesi hâlinde, savcı kararını yirmi dört saat içinde yetkili ve görevli yargıcın onayına sunacak yargıç da savcının kararını almasından itibaren bu konuda yirmi dört saat içinde karar verecektir. Savcının kararının yirmi dört saat içinde onaylanmaması yani yargıç tarafından savcının kararı alındıktan itibaren yirmi dört saat sonunda olumlu ya da olumsuz bir karar verilmemesi hâlinde, savcının kararı onaylanmamış sayılacak ve söz konusu karar, savcı tarafından kaldırılacaktır. Koruma tedbiri olarak verilen erişimin engellenmesi kararına 5271 sayılı CMK'nın 267 vd. maddelerine göre itiraz edilmesi mümkündür.

Öncelikle belirtilmelidir ki, 5651 sayılı Yasa yürürlüğe girene kadar yasal bir dayanağı olmaksızın, yargıçlar tarafından olması gerektiği gibi, adeta özel hukuk yargıcının görevi olan *"hukuk yaratılarak"* verilen erişimin engellenmesine yönelik tedbir kararının yasal bir zemine oturtulması, olumlu bir gelişmedir. Böylelikle uygulama yasal hale getirilmektedir. Böyle önemli bir kararın verilmesi yetkisinin yargıçlara verilmesi diğer bir olumlu gelişmedir. Gecikmesinde sakınca bulunan

12 Dülger, s.777.

hâllerin hangisi olduğunu ise cumhuriyet savcısı kendisi belirleyecek ve buna göre kendisi karar verecektir. Ancak 8. maddenin 1. fıkrasında belirtilen suç tipleri açısından gecikmesinde sakınca bulunan hâllerin gerçekleşmesi olasılığı zayıf görülmektedir. Çünkü kasten öldürme, organize suçlar ya da terör suçları gibi anında müdahale edilmesi gereken suç tipleri bu listede yer almamaktadır. Buna rağmen savcının aldığı bu kararın da yargıç denetimine tabi tutulması ve hem bu kararın gönderilmesinin hem de kararın denetlenmesinin yirmi dört saatlik kısa sürelere tabi tutulması, yargıcın karar vermediği duruma da bir sonuç bağlanarak bunun tedbirin kaldırılması anlamına geldiğinin belirtilmesi bu düzenlemeyi iyi bir düzenleme hâline getirmektedir.[13]

5.2.3. Uygulanacak Yöntem

Yasanın 8. maddesinin 3. fıkrasına göre, dosyanın soruşturma ya da kovuşturma aşamasında bulunmasına göre, yargıç, mahkeme veya cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının bir örneği, gereği yapılmak üzere başkanlığa gönderilecektir. Bu sayede başkanlık tarafından ilgili karar da belirtilerek tüm erişim sağlayıcılara konu hakkında yazılı bilgi verilecek ve kararda gösterilen adreslere erişimin engellenmesine ilişkin kararın uygulanması sağlanacaktır. Bu kararın gereği başkanlık tarafından erişim sağlayıcılara bildirim yapıldıktan sonra derhal ve en geç kararın bildirilmesi anından itibaren yirmi dört saat içinde yerine getirilecektir (5651 sayılı yasa m.8/5).

Buna göre kararların doğrudan erişim sağlayıcılara gönderilmesi mümkün değildir. Erişim engelleme kararı TİB tarafından erişim sağlayıcılara bildirilecektir. Uygulama Yönetmeliği'nde bu kararların erişim sağlayıcılara elektronik ortamda bildirilmesi kabul edilmiştir. Bu şekilde hızlı bir şekilde içerik, yer veya erişim sağlayıcılara ulaşılarak kararın yerine getirilmesi sağlanabilmektedir.

Uygulama Yönetmeliği'nin 15. maddesinde erişim engellemekararlarında belirtilmesi gereken hususlara yer verilmiştir. Buna göre, kararı veren merciin adı, soruşturma veya mahkeme esas numarası, tedbirin hangi suç için istendiği ve yeterli şüphe sebeplerinin neler olduğu, suça ilişkin bilgilerin bulunduğu URL ve alan adı, yer sağlayıcıya ait IP adresi ve alan adı veya IP adresi olarak erişim engelleme yönteminin kararda belirtilmesi gerekmektedir. Web sitelerine erişimin engellenmesi için farklı tekniklerin kullanılabileceği belirtilmiştir. Ne yasada ne de yönetmelikte hangi tekniğin kullanılması gerektiğine ilişkin bir düzenleme bulunmaktadır. Dolayısıyla kararı veren yargıç internet iletişimi özgürlüğünü en az kısıtlayan ve başkalarının haklarına en az zararı veren yöntemi seçerek kararını vermelidir.[14]

5.2.4. Tedbir Kararının Kalkması

Cumhuriyet savcılığı tarafından yapılan soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz hale gelecektir. Bu durumda savcılık söz konusu takipsizlik kararını ve koruma tedbirinin hükümsüz kaldığına ilişkin bir yazıyı başkanlığa gönderecektir, başkanlık da bu durumu erişim sağlayıcılara bildirerek engellemenin kaldırılmasını sağlayacaktır.

5651 sayılı Yasanın 8. maddesinin 2. fıkrasına göre, koruma tedbiri olarak

13 Dülger, s.778.

14 Dülger, s.779.

verilen erişimin engellenmesi kararlarına karşı 5271 sayılı CMK hükümlerine göre itiraz edilmesi mümkündür. Ayrıca 8. maddenin 13. fıkrasında, uygulanmak üzere TİB'e gönderilen kararlara, TİB tarafından da itiraz edilebileceği düzenlenmiştir.

Uygulama Yönetmeliği'nde bu kararlara karşı TİB dışında 5271 sayılı CMK hükümlerine göre ilgililer tarafından da itiraz edilebileceği öngörülmekle beraber, ilgililerin kimler olduğu yönünde açıklayıcı bir ifade bulunmamaktadır. Buna göre, ilgili kişi ibaresinden hukuksal çıkarları etkilenen kişilerin anlaşılması gerektiği ve erişim engelleme kararına karşı bir web sitesinin kullanıcılarının dahi itiraz hakkının bulunduğu söylenebilecektir.

Kovuşturmaya yer olmadığı kararına CMK'nın 173. maddesi gereğince itiraz edilmesi ve itiraz sonucunda kamu davası açılmasının istenmesi hâlinde erişimin engellenmesi tedbirinin durumu ne olacaktır? 5651 sayılı yasanın 8. maddesinin 7. fıkrasında kovuşturmaya yer olmadığı kararının verilmesi hâlinde başkaca bir karar verilmesine gerek kalmaksızın daha önce verilmiş olan erişimin engellenmesi kararının kendiliğinden hükümsüz hale geleceği açıkça belirtilmektedir. Dolayısıyla savcının CMK'nın 172. maddesi gereğince kovuşturmaya yer olmadığı kararı vermesi halinde sonradan itiraza konu olsa da söz konusu tedbir kendiliğinden kalkacaktır. İtiraz sonucu verilen karar üzerine savcının iddianame düzenleyerek dava açması hâlinde ise eğer bu tedbire yeniden gerek duyulursa yukarıda açıklanan yöntem izlenerek karar verilebilecektir; ancak bu ikinci ve farklı bir tedbir kararı olacaktır.

Yukarıda açıklanan kovuşturmaya yer olmadığı kararındaki duruma benzer biçimde, yapılan kovuşturma sonucunda fail hakkında beraat kararı verilmesi hâlinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalacaktır. Bu durumda da beraat kararının bir örneği başkanlığa gönderilecek ve başkanlık yukarıda açıklandığı biçimde gereğini yapacaktır. Ancak yapılan yargılama sonucunda gerçekleşen eylemin gerçekten suç olduğu ancak bunu yapanın yargılanan sanık olmadığı anlaşılırsa ne olacaktır? Yargılamada birden çok kişi sanık durumunda ise ve bunlardan bazıları beraat ederken bazıları üzerlerine atılı suçlardan mahkûm olursa tedbirin akıbeti ne olacaktır? İşte bu madde düzenlenirken adeta yalnızca eylem yargılanıyormuş gibi ya da tek bir fail yargılanacakmış gibi düzenleme yapılmıştır; bu ise sorunlara yol açabilecek niteliktedir. Yukarıdaki soruların yanıtları ise şöyle olmalıdır:

Birinci olasılıkta hukuka aykırı eylem varlığını devam ettirdiği ancak sanık beraat ettiği için bu durum kararda belirtilmeli ve savcılık tarafından farklı bir hazırlık numarası üzerinden soruşturma yürütülmelidir, 5651 sayılı Yasanın 8. maddesinin 8. fıkrası gereğince beraat kararı sonucunda tedbir kararı kendiliğinden hükümsüz hale geleceği için de bu yeni soruşturmaya birlikte yeniden gerekli yöntem izlenerek erişimin engellenmesi kararı talep edilecektir.

İkinci olasılıkta ise, içeriği 8. maddenin 1. fıkrasında belirtilen suçları oluşturan yayın nedeniyle sanıkların mahkûm olmaları hâlinde koruma tedbiri devam edecektir. Ancak bu da ceza muhakemesi hukukuna uymayan bir durum oluşturmaktadır. Çünkü koruma tedbirleri varlıklarını soruşturma ve kovuşturma evresi boyunca sürdürürler, zîra bunların amacı soruşturma ve kovuşturmanın daha çabuk ve etkin yapılmasını sağlamaktır. Tedbirlerin devam etmesi isteniyorsa, bunun mahkeme tarafından verilen hükümde yaptırım ya da güvenlik tedbiri olarak belirtilmesi gerekir. Erişimin engellenmesi tedbiri de failin ya da faillerin tamamının beraati hâlinde kendiliğinden kalkacaktır; ancak mahkûmiyet Hâlinde verilen karar ne olacaktır? Çünkü yargılamayı

sonlandıran beraat ya da mahkûmiyet gibi kararlarla koruma tedbirleri kalkacaktır. İşte bunun için bu tedbirin devamı niteliğinde yeni bir güvenlik tedbiri düzenlenmelidir. Yasanın bu haliyle mahkûmiyet hâlinde erişimin engellenmesi tedbirinin akıbetinin ne olacağı hususunda yasal boşluk bulunmaktadır. Koruma tedbirleri temel hak ve özgürlükleri kısıtladıkları için aynen suç normlarında olduğu gibi suçta ve cezada yasallık ilkesi gereğince koruma tedbirlerine ilişkin boşlukların yorum ya da kıyas yoluyla doldurulması mümkün değildir.

Konusu yasanın 8. maddesinin 1. fıkrasında sayılan suçları oluşturan içeriğin yayından çıkartılması halinde, erişimin engellenmesi kararı soruşturma evresinde cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılacaktır (5651 sayılı yasa m.8/9). Bunun için tedbirden etkilenen tarafların başvurusu aranmamıştır, savcı ya da mahkeme bu kararı kendiliğinden alabilecektir; ancak bu konuyla ilgili olanların talepte bulunmalarına da engel oluşturmamaktadır. Koruma tedbirinin kaldırılması konusunda savcının kendiliğinden karar vermesi uygun olmamıştır; nasılki, bu karar savcının talebi üzerine yargıç tarafından veriliyorsa ya da gecikmesinde sakınca bulunan hallerde yargıcın onayına sunuluyorsa, söz konusu kaldırmaya ilişkin karar da yargıcın kararıyla ya da onayıyla gerçekleştirilmelidir. Ancak bu düzenleme de bireylerin haklarını koruyan amaca uygun ve demokratik bir düzenlemedir.[15]

5.2.5. Yaptırım

Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcıların sorumluları, eylem daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adlî para cezası ile cezalandırılacaklardır. Yer veya erişim sağlayıcılar 8. maddenin 5. fıkrasına göre, başkanlık tarafından kendilerine bildirilen erişimin engellenmesi kararının gereğini, bu bildirimden itibaren en geç yirmi dört saat içinde yapmadıkları takdirde 8. maddenin 10. fıkrasına göre adlî para cezasına mahkûm olacaklardır. Erişimin engellenmesi kararının yerine getirilebilmesi için bu şekilde etkili çözümler alınmış olması yasanın uygulanabilirliği ve etkililiği açısından yerinde bir düzenlemedir.[16]

5.3. İdari Tedbir Olarak Erişimin Engellenmesi

5.3.1. Yasal Dayanak

5651 sayılı Yasanın 8. maddesinin 4. fıkrasında, idari bir tedbir olarak internet erişiminin engellenmesi hali düzenlenmiştir. Bunun idari bir tedbir olarak düzenlenmiş olduğu yer aldığı fıkranın başlığı ya da içeriğinden değil, 11. fıkradaki düzenlemeden anlaşılmaktadır. Buna göre 11. fıkrada *"idari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde"* denildiği ve daha önceki fıkralarda 2. fıkradaki düzenlemenin ceza muhakemesi koruma tedbiri niteliğinde olduğu belirtildiği için, 4. fıkradaki düzenlemenin idari bir tedbir olduğu anlaşılmaktadır. Tekrar belirtilmelidir ki, bu tarz düzenleme yasa yapma tekniği açısından son derece olumsuz bir örnektir; çünkü yasa maddesi adeta bulmaca haline getirilmiştir.[17]

15 Dülger, s.779.

16 Dülger, s.781.

17 Dülger, s.785.

5.3.2. Kararı Verebilecekler

Buna göre içeriği 8. maddenin 1. fıkrasında belirtilen suçları (5237 sayılı TCK m. 84 *intihara yönlendirme*, m.130/1 *çocukların cinsel istismarı*, m.190 *uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma*, m.194 *sağlık için tehlikeli madde temini*, m.226 *müstehcenlik*, m.227 *fuhuş*, m.228 *kumar oynanması için yer ve imkân sağlama, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanununda yer alan suçlar)* oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği 1. fıkranın (a) bendinin (2) ve (5) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı resen Telekomünikasyon İletişim Başkanlığı tarafından verilecektir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yapılması istenecektir.

Bu çalışmanın bütününde belirttiğimiz üzere, böyle bir yetkinin idareye verilmemesi gerekir, zîra bu yetki, idarecilerin inisiyatiflerine göre kolaylıkla keyfi kullanımlara dönüşebilecektir. Ancak öğretide bazı yazarlar bir konuda hem adlî hem de idari makamların yetkilendirilmesinin yerinde olmadığını belirtmekle beraber, hukuka aykırı içeriğe ilişkin hızlı hareket etmek zorunluluğu olduğu için bu tür yetkilerin birçok demokratik düzende TİB benzeri idari kurumlara verildiğini belirtmektedirler. Biz yazarların bu görüşüne katılmıyoruz. Hukuka aykırı içeriğin kaldırılması için adlî makamların da hızlı hareket etmesi mümkün ve gerekli olduğu gibi, bu uygulamanın bir başka demokratik düzende olması, bizatihi bu uygulamanın demokratik olduğu anlamına gelmemektedir.[18]

5.3.3. İdari Tedbir Olarak Erişim Engellemenin Hukukî Niteliği

İdare Hukukunda *"idari tedbir"* adıyla ayrı bir hukukî işlem bulunmamaktadır; dolayısıyla bu kendine özgü bir hukukî işlem ya da eylem değildir. Bu yasada düzenlenen erişimin engellenmesi idari tedbiri, idarenin bir kamu hizmeti olan kamu güvenliğini sağlamak amacıyla vereceği tek yanlı *"birel-öznel"* işlemdir. Buna göre başkanlığın alacağı bu tür kararlar idare hukukunun kurallarına tabi olacak ve bu kararlara karşı itiraz mercii de idari yargı olacaktır.

Ancak belirtilmelidir ki, bu düzenleme hukuka aykırıdır ve amaca uygun değildir. Yargılama makamlarının konusuna giren bir alanda idarenin yetkilendirilmesi açık bir yetki gaspı oluşturmaktadır. Fıkrada 8. maddenin 1. fıkrasında belirtilen suçu oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında olması hâlinde erişimin engellenmesi kararının resen idari bir yapı olan TİB tarafından verileceği belirtilmektedir. Ayrıca içerik ve yer sağlayıcı yurt içinde bulunsa bile içeriği 5237 sayılı TCK m.130/1'de yer alan çocukların cinsel istismarı ve m.226'da yer alan müstehcenlik suçlarını oluşturduğu takdirde erişimin engellenmesi kararının resen başkanlık tarafından verileceği düzenlenmektedir. Aslında bir muhakeme hukuku konusu olan tedbir niteliğindeki önlemlere hem idari yargılama hukukunda (yürütmenin durdurulması) hem medeni yargılama hukukunda (ihtiyati tedbirler ve delil tespit işlemleri) hem de ceza muhakemesi hukukunda (tutuklama, arama vd.) rastlanmaktadır. Yargılama faaliyetinin gerek sağlıklı biçimde yapılabilmesi ve gerek sonuçta verilen kararların uygulanabilmesi için henüz yargılama faaliyeti devam ederken alınan önlemler söz konusu tedbirleri oluşturmaktadır. Ayrıca bu tedbirlerin iki özelliği bulunmaktadır: *araç olma ve geçici olma.* İdare açısından da idari tedbir

18 Dülger, s.785.

niteliğinde düzenleyici işlemlerin yapılması mümkündür. Örneğin gösteri yürüyüşü yapılacak güzergâhın, yürüyüşün güvenliği için polis tarafından araç trafiğine kapatılması bir idari tedbirdir. Ancak bu idari tedbirler de hem amaca ulaşmak için araç olma hem de geçici olma özelliğini göstermektedirler. Ancak idare tarafından erişimin engellenmesine yönelik bu düzenlemenin araç olma özelliği ve geçici olma özelliği bulunmamaktadır. Söz konusu fıkrada idare erişimin engellenmesi kararı alırken bunun neyin aracı olduğu belirtilmemiştir. Oysa koruma tedbiriniteliğindeki erişimin engellenmesi kararı soruşturma ve kovuşturma faaliyeti ile ilgili olarak düzenlenmiştir. İdari tedbir niteliğindeki erişimin engellenmesi kararının ne zaman sona ereceği maddede belirtilmemektedir; oysaki koruma tedbiri niteliğindeki erişimin engellenmesi kararı için bunlar açık bir biçimde düzenleme konusu yapılmıştır. İşte bunlar yapılan düzenlemenin ne kadar hatalı olduğunu açık bir biçimde ortaya koymaktadır.

Ayrıca 5651 sayılı yasanın 8. maddesinin 4. fıkrasında düzenlenen idari tedbirin niteliğine bakıldığında bunun yargılama faaliyetine ilişkin bir tedbir olduğu, dolayısıyla bunun aslında bir koruma tedbiri olduğu görülmektedir. Maddenin 2. ve 3. fıkralarında soruşturma ve kovuşturma makamlarına belli suçlar için koruma tedbiri niteliğinde erişimin engellenmesi tedbiri alınabilmesi yetkisi verilmiş ve bunun yöntemi düzenlenmiştir. Aynı maddenin 4. fıkrasında ise yönetimin daha düzgün yapılabilmesi amacına yönelik değil, ceza muhakemesi koruma tedbirinde yer alan aynı suç tipleri için yalnızca biraz daha farklı koşullarda tedbir kararı alınması amacıyla idareye karar alma yetkisi verilmiştir. Oysa içerik veya yer sağlayıcının yurt dışında olması halinde ve içeriğin çocukların istismarı ya da müstehcenliğe ilişkin olması hâlinde de yargılama organlarının karar alması pekâlâ mümkündür. Zaten 2. fıkrada gecikmesinde sakınca olan hallerde savcıya karar verme yetkisi tanınmıştır. Temel hak ve özgürlüklere ilişkin bu kadar önemli bir konuda yargılama makamları dışında idareye yetki verilmesi anlamsız, anti demokratik ve hukuk dışıdır.

Bu konuda belirtilmesi gereken önemli bir konu da, koruma tedbiriolarak verilen erişimin engellenmesi kararı ile idari tedbir olarak verilen erişimin engellenmesi kararında izlenen yöntemler arasındaki farktır. Koruma tedbiri olarak alınan kararın kural olarak mahkeme tarafından bu kararın verilebileceği, fakat gecikmesinde sakınca bulunan hallerde savcı tarafından verilebileceği ancak savcı tarafından verilen kararın en geç yirmi dört saat içinde yargıç onayına sunulacağı, yargıcın doğrudan bu kararı onaylamadığını açıklaması ya da yirmi dört saat içinde bu konuda karar vermemesi durumunda kararın kendiliğinden ortadan kalkacağı düzenlenmiştir. İdari tedbir olarak alınan karar ise ancak yasada belirtilen istisnai durumlarda (ki internetin yapısı gereği bu istisnadan çok kural hâline gelmiştir) doğrudan başkanlık tarafından bu karar alınacak ve hiçbir yargısal makamın onayına sunulmayacaktır. Bu anlaşılması güç, internetin yapısına kesinlikle uymayan ve temel hak ve özgürlüklere her an müdahalede bulunulabilmesini sağlayacak son derece anti demokratik bir düzenlemedir.

Her ne kadar idari ve adlî görevleri olsa ve görev açısından idareye bağlı olsa da her şeyden önce "bir hukukçu olan" ve yargısal anlamda faaliyetleri de bulunan savcının vermiş olduğu karar dahi en geç yirmi dört saat içinde yargıç onayına sunulurken; hukuk eğitimi almamış olması kuvvetle muhtemel olan, yargısal hiçbir görevi olmayan ve idarenin ajanı olan kişilerden oluşan TİB tarafından böyle bir kararın alınması ve bunun hiçbir makamın denetimine tabi tutulmaması son derece hatalı bir düzenlemedir. Bu karar aleyhine idari yargıda iptal davası açılması ve yürütmenin

durdurulması kararı istenmesi mümkün olsa da bu mahkemelerde kısa sürede karar alınması pek mümkün olmamaktadır. Hele iletişimle ilgili bir konuda yayının dakikalarca kesilmesi dahi önemli sorunlara neden olabilmektedir. Koruma tedbiriolarak verilen karar ile ilgili yirmi dört saatlik düzenlemelerle, idari yargı yolu açık olan bu düzenleme zamansal açıdan da büyük bir çelişkiyi barındırmaktadır.[19]

5.3.4. Uygulanacak Yöntem

Yasanın 8. maddesinin 4. fıkrasına göre, başkanlık tarafından verilen erişimin engellenmesi kararı tüm erişim sağlayıcılara bildirilecek ve kararda gösterilen adreslere erişimin engellenmesine ilişkin kararın uygulanması sağlanacaktır. Bu kararın gereği başkanlık tarafından erişim sağlayıcılara bildirim yapıldıktan sonra derhal ve en geç kararın bildirilmesi anından itibaren yirmi dört saat içinde yerine getirilecektir (5651 sayılı yasa m.8/5).

Ayrıca başkanlık tarafından yasanın 8/4 maddesi gereğince alınmış idari tedbir niteliğindeki erişimin engellenmesi kararının konusunu oluşturan yayını yapanlarının kimliklerinin belirlenmesi halinde, başkanlık tarafından cumhuriyet savcılığına suç duyurusunda bulunulacaktır. Bu düzenleme ceza yasası ve ceza muhakemesi kurallarıyla çelişmektedir. Çünkü bu düzenleme yapıldığında yürürlükte olan 5237 sayılı TCK'nın 278. maddesine göre, işlenmekte olan bir suçun yetkili makamlara bildirilmemesi suç olarak tanımlanmaktadır. Burada işlenmekte olan suçla kastedilen suç oluşturan eylemin bilinmesidir; yoksa failin kimliği hakkında bilgi sahibi olunması gerekmemektedir. Faili bulmak ve kimliğini tespit etmek soruşturma makamlarının işidir. Ceza muhakemesi açısından da şikayette ya da suç duyurusunda bulunulacağı zaman failin kimliğinin ve açık adresinin bildirilmesi gerekmemektedir. Failin yalnızca eşkalinin verilmesi dahi yeterli olduğu gibi faili meçhul olarak yalnızca eylemin bildirilmesi geçerli bir suç duyurusu ya da şikayet olarak kabul edilmektedir. Buna göre başkanlık tarafından verilen erişimin engellenmesi kararının konusunun suç olması düzenleme gereği kaçınılmazdır.Dolayısıyla yukarıda yapılan açıklamalar ışığında başkanlık eylemi öğrenir öğrenmez (tabi ki faili öğrenmişse bunu da) elindeki tüm bilgilerle yetkili savcılığa suç duyurusunda bulunmak zorundadır. Zaten TCK'nın düzenlemesi karşısında bu konuda bir daha düzenleme yapılması gereksizdir. Ancak fıkrada bu suç duyurusunda bulunmanın failin kimliğinin belirlenmesi şartına bağlanması açıkça TCK ve CMK ile çelişki oluşturmakta, hatta başkanlık açısından Anayasa Mahkemesi tarafından iptal edilmeden önce TCK'nın 278. maddesinde tanımlanan suçun işlenmesini zorlaştırmaktadır.

Burada "söz konusu kimliklerin belirlenmesi zaten başkanlık tarafından yapılacaktır" gibi bir yanıt verilebilecek olsa da bu yanıt da hatalı olacaktır. Birincisi failin kimliği tespit edilmeden de soruşturma yürütülmekte, örneğin hem failin kimliği araştırılmakta hem de eylemle ilgili deliller toplanmaya çalışılmaktadır. İkincisi ise, soruşturma makamları bu eylemleri gerçekleştiren faillerin kimliklerinin tespit edilmesini mutlaka başkanlıktan isteme zorunluluğunda değildirler. Bu araştırma, örneğin polisin ilgili birimleri tarafından yerine getirilebileceği gibi, bu konuyla ilgili diğer kurum ya da kuruluşlardan da bu talepte bulunulabilecektir. Bu konudaki takdir ve seçim hakkı soruşturma makamlarında bulunmaktadır. Sonuç olarak 5651 sayılı yasanın 8. maddesinin 6. fıkrası TCK ve CMK ile çelişen hatalı bir düzenleme olarak düzenlenmiştir.[20]

19 Dülger, s.786.

20 Dülger, s.788.

5.3.5. Yaptırım

İdari tedbir olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen erişim sağlayıcılara on bin TL'den yüz bin TL'ye kadar idari para cezası verilecektir. Ayrıca idari para cezasının verildiği andan itibaren yirmi dört saat içinde kararın yerine getirilmemesi hâlinde başkanlığın talebi üzerine kurum tarafından erişim sağlayıcılığı hizmeti verilmesine ilişkin yetkilendirmenin iptaline karar verilebilecektir. Buna göre erişim sağlayıcılar 8. maddenin 5. fıkrasına göre, başkanlık tarafından kendilerine verilen erişimin engellenmesi kararının gereğini, bu bildirimden itibaren en geç yirmi dört saat içinde yapmadıkları takdirde 8. maddenin 11. fıkrasına göre idari para cezası ile cezalandırılacaklar, idari para cezası kesildikten sonra yirmi dört saat için hâlâ erişimi engellemedilerse bu kez de yetkileri iptal edilebilecektir.

Erişimin engellenmesi kararının yerine getirilebilmesi için bu şekilde etkili çözümler alınmış olması yasanın uygulanabilirliği ve etkililiği açısından yerinde bir düzenlemedir. Ancak, koruma tedbiri olarak erişimin engellenmesi kararı için yetki iptali gibi bir yaptırımın öngörülmemiş olmasına rağmen, idari tedbir için böyle ağır bir yaptırımın hem de erişim sağlayıcı için öngörülmüş olmasının mantıksal bir açıklaması yoktur. Bu düzenleme söz konusu idari tedbiri bir tedbir olmaktan çıkarmış adeta başlı başına bir kural ve sonucunu da yaptırım hâline getirmiş ve bu yapılırken de hiçbir orantı gözetilmemiştir.

Yasanın 8. maddesinin 12 nolu fıkrasında ise yasada tanımlanan kabahatler dolayısıyla başkanlık veya kurum tarafından verilen idari para cezalarına ilişkin kararlara karşı 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre yasa yollarına başvurulacağı belirtildiği için, 11. maddeye göre idari para cezası verilmesi ya da kurum tarafından yetkilendirmenin iptaline karar verilmesi halinde bu kararların iptali için altmış gün içinde idari yargıda iptal davası açılması mümkündür.[21]

5.4. İçeriğin Yayından Kaldırılması ve Erişimin Engellenmesi

5651 sayılı Yasa'nın *"içeriğin yayından çıkarılması ve erişimin engellenmesi"* başlıklı 9. maddesinde, internet aracılığıyla iletilen içerik nedeniyle hakları ihlal edilen kişilerin söz konusu içeriklerin yayından kaldırılması yönelik düzenleme yapılmıştır. Uygulamada çok sık karşılaşılan ve *"uyar – kaldır yöntemi"* denilen bu uygulama büyük oranda başarılı sonuçlara ulaşılmasını sağlamıştır.

Bu maddeye göre, internette yer alan içerik nedeniyle haklarının ihlal edildiğini iddia eden kişi, içerik sağlayıcısına, buna ulaşamadıkları takdirde yer sağlayıcısına başvurarak kendilerine ilişkin içeriğin yayından çıkartılmasını isteyebilceği gibi kişinin doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini talep edebilir. İçerik ve yer sağlayıcı söz konusu talebin kendilerine ulaştıktan en geç yirmi dört içinde cevaplandırır.

Bu, uygulamaya son derece elverişli bir düzenleme olmasına rağmen iki noktada sıkıntı söz konusu olmaktadır. Bunlardan ilki söz konusu istem, yalnızca yurt içinden içerik sağlayan ya da yer sağlayanlar için uygulama alanı bulabilmektedir. Çünkü yurt dışından bu eylemi gerçekleştirenler hem yasanın uygulama alanı açısından, hem de bunlara yaptırım uygulanmasının olanaksızlığı bakımından söz konusu yasanın kapsamı dışında kalmaktadırlar. Ancak bu yasa koyucunun elinde

21 Dülger, s.789.

olan bir neden olmadığı gibi maddenin düzenlenişi açısından da bir sakatlık değildir. Bu durum konunun uluslararası boyutunu ortaya koymakta ve tüm ülkelerde benzer düzenlemelerin gerekliliğini ve ülkeler arası iş birliğinin zorunluluğunu göstermektedir.

İkinci sıkıntı yaratan nokta ise içerik sağlayıcıya ulaşmanın mümkün olmaması hâlinde talebin yer sağlayıcıyayöneltilmesi hâlidir; çünkü yer sağlayıcının, hizmet sunduğu içeriklere müdahalede bulunma yetkisi bulunmamaktadır. Aksine hareket edilmesi TCK'nın 244. maddesinde düzenlenen "bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunun" gerçekleşmesine yol açabilecektir. Her ne kadar 5651 sayılı Yasanın 9/1. maddesinin TCK'nın 244. maddesinde düzenlenen suç için içerik sağlayıcılar açısından bir hukuka uygunluk nedeni oluşturduğu söylenebilecekse de bu yalnızca hak ihlaline neden olan içeriğin kaldırılması için geçerlidir. Bunun aksine olarak özellikle yer sağlayıcıların web sitesinin içeriğine müdahale etmek için gerekli olan şifrelere sahip olmadıkları gerekçesiyle hak ihlaline neden olan içerikle beraber bu içeriğin yer aldığı tüm web sayfasını kaldırarak erişimi engellemeleri hukuka uygun olmayacaktır. Bu durumda 5651 sayılı Yasanın 9/1. maddesi, hukuka uygunluk nedeni oluşturmayacağı için yer sağlayıcılar açısından cezai sorumluluk söz konusu olacaktır. Dolayısıyla 5651 sayılı Yasanın 9/1. maddesinin uygulanmasında yalnızca hak ihlal eden içerik yayından çıkarılmalıdır.

Kişilik hakkının ihlal edildiğini iddia eden kişinin doğrudan sulh ceza mahkemesine başvurması halinde, hâkim başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlayacaktır. Sulh ceza hâkiminin bu kararına karşı 5271 sayılı CMK'nın 267 vd. maddelerine göre itiraz edilmesi mümkündür.

Yukarıda belirtilen çekince bu fıkradaki düzenleme açısından da geçerlidir. İçerik ve/veya yer sağlayıcının yurt dışında olması hâlinde neye karar verilecektir, karar alınsa dahi bunun uygulaması nasıl olacaktır? Söz konusu içerik ve/veya yer sağlayıcının yurt dışında olması ve verilen kararın uygulanamaması halinde hak ihlali içeren içeriklere erişim mümkün olabilecek midir? Yukarıda belirtildiği üzere, 8. maddede düzenlenen erişimin engellenmesi kararında yer alan eksiklikler burada etkisini göstermektedir. Çünkü böyle bir durumda, hak ihlali oluşturan içerik hakkında erişimin engellenmesi kararı verilebilmeli; bunun için de söz konusu maddede suçlar sınırlanmamalı ya da hakaret suçu da bu kataloğun içine alınmalıydı.

Bu maddeyle ilgili uygulamada en sık karşılaşılan sorun, hakkı ihlal edilen kişinin *"uyarısını nasıl yapması gerektiği"* konusunda yaşanmaktadır. Yasa maddesinde bu konuda bir şekil şartı ya da biçim bulunmamaktadır. Madde 9'da haklarının ihlal edildiğini iddia eden kişinin, içerik sağlayıcısına, buna ulaşılmaması halinde ise yer sağlayıcısına *başvurması, istemesi ve talepte bulunmasının* gerekli ve yeterli olduğu belirtilmiştir. Bu bağlamda uygulamada söz konusu internet kişilerine bir elektronik posta gönderilmesi yeterli olmakta; mahkemeye başvurulması halinde ise söz konusu elektronik posta tek başına 9. maddenin işletilmesi için yeterli sayılmaktadır. Ancak bazı sulh ceza yargıçları tarafından söz konusu uyarının *"noterden gönderilen ihtarname"* ile yapılması istenilmekte aksi hâlde şekil şartı gerçekleşmediği gerekçesiyle başvurular reddedilmektedir. Bu tamamen hukuka ve yasaya aykırı bir uygulamadır. Öncelikle yasada böyle bir şekil şartı bulunmamaktadır. Yasada olmayan bir şekil şartının, kişinin hakkını korumak için düzenlenen bir yasa yolunun kullanımını daraltacak şekilde yorumlanması ve uygulanması ise, mümkün değildir. Öte yandan kişinin hakkında yüz farklı sitede hakaret içeren haberler olması ve bunların hepsini kaldırmak istemesi hâlinde, tek sayfalık bir ihtarnamenin noter

kanalıyla gönderilmesi hâlinde sayfa başına yaklaşık yüz TL'lik bir maliyeti olduğu göz önünde bulundurulduğunda bunun maliyeti haksızlığa uğrayan kişi için on bin TL olacaktır. Bireyin hakkı ihlal edilmiş iken, bu hakkı kullanmak için bir de böyle bir maliyete katlanmak zorunda bırakılması mülkiyet hakkının da ihlal edilmesi ve etkin iç hukuk yolu olmaması anlamına gelecektir. Bu da açık bir hukuka aykırılıktır. Ayrıca artık mahkemeler ve diğer resmi kuruluşlar, bireylere olan güvensizliği de bir yana bırakmalıdırlar.

6 ULUSLARARASI İSTİNABE

6. ULUSLARARASI İSTİNABE

6.1. Genel Olarak Uluslar arası İstinabe

Bilişim suçları ilk ortaya çıktıklarında yalnızca ulus devletin sınırları içinde işlenmekteydi.Ancak internetin ortaya çıkması ve yaygınlaşmasıyla bu suçlar uluslararası bir boyut kazanmıştır. İnternetin yaygınlaşması zaten ticaret alanında kendi hissettiren küreselleşmeyi daha da hızlandırmış, küreselleşme de internet kullanımını zorunlu hâle getirmiş ve böylelikle bir sarmal hâlinde birbirlerini tetiklemişlerdir. Özetle, konunun uluslararası boyutta önem kazanması küreselleşmenin hızlanması ile birlikte olmuştur; çünkü uluslararası suçluluk, küreselleşme sürecinin bir parçasıdır. Buna bağlı olarak da bilişim suçları uluslararası ceza hukukunun ilgi alanına girmiştir.

Bilişim suçlarının en önemli özelliklerinden birini de bu suçların genellikle sınır aşan bir biçimde işlenmesi ve buna bağlı olarak uluslararası bir boyutunun olmasıdır. Dolayısıyla günümüzde bilişim suçlarıyla ilgili olarak uluslararası kuruluşlar ve çalışmalar olduğu gibi, çok ciddi hukuksal düzenlemeler de bulunmaktadır. Nitekim ulusal hukuklarda konuyla ilgili olarak yapılan düzenlemelerin çoğu ya uluslararası düzenlemelerden alınmış ya da bunlara uyumlu hale getirilmiştir. Özellikle Avrupa Siber Suç Sözleşmesi'nin yürürlüğe girmesinden sonra taraf ülkeler için durum tam bu şekildedir.

Aslında bilişimsuçları, küresel bir nitelik taşımaktadır. Çünkü özellikle hukuka aykırı ekonomik çıkar elde etmek ya da gizli verileri elde etmek amacıyla işlenen bilişim suçları genellikle uluslararası süreçlerden geçmektedir.

Bu suçların uluslararası boyutunun olması, bunların genellikle sınır aşan biçimde işlenmesi ve dolayısıyla uluslararası ceza hukukunun bir parçası olması nedeniyle; bilişim suçlarının ve bunlarla mücadelenin, *"ceza yasalarının uygulanma alanı sorunu"* ve *"uluslararası adlî yardımlaşma"* konuları dikkate alınmaksızın etkin bir biçimde gerçekleştirilmesi mümkün değildir. Bu suçlarla ilgili olumlu olan gelişme ise, bu suçların ciddiyetine varan uluslararası toplumun, bu suçlarla mücadele için uzun bir süreden beri uluslararası boyutta işbirliğine başlamış olmasıdır.[1]

6.2. Türkiye Açısından Uluslararası Adlî Yardımlaşmanın Hukukî Dayanakları :

Türkiye açısından uluslararası adlî yardımlaşma; çok taraflı sözleşmeler veya ikili antlaşmalar, bunların bulunmaması hâlinde uluslararası teamül hukuku kuralları veya karşılıklılık ilkesi çerçevesinde yürütülmektedir.

Çok Taraflı Sözleşmeler

Avrupa Konseyi üyesi olarak Türkiye uluslararası adlî yardımlaşma konusunda hükümler içeren; Ceza İşlerinde Karşılıklı adlî Yardımlaşma Avrupa Sözleşmesi, Ceza Yargılarının Milletlerarası Değeri Konusunda Avrupa Sözleşmesi veya Ceza Kovuşturmalarının Aktarılması konusunda Avrupa Sözleşmesi gibi çok sayıda uluslararası sözleşmenin tarafıdır.

Uluslararası adlî yardımlaşma işlemlerinde en fazla başvurduğumuz çok

1 Dülger, s.167.

taraflı sözleşme CİKAYAS kısaltmasıyla da tanınan Ceza İşlerinde Karşılıklı adlî Yardım Avrupa Sözleşmesidir.

Avrupa Konseyi'nin 30 nolu Sözleşmesi olan bu Sözleşme 1959 yılında imzaya açılmış olup otuz maddeden oluşan bir çerçeve sözleşme niteliğindedir. Türkiye 1968 yılında bu sözleşmeye taraf olmuştur.
Avrupa Ülkelerinin hepsi CİKAYAS'a taraf olmakla birlikte Azerbaycan, Ermenistan, İsrail, Güney Kore, ve Brezilya gibi Avrupa ülkesi olmayan bazı devletler de anılan Sözleşmeye taraftır.

İkili Antlaşmalar

CİKAYAS'a taraf olmayan ve aramızda ikili antlaşma olan devletlerleolan adlî yardımlaşma işlemleri ikili antlaşmalardaki hükümlere göre yerine getirilir. Aramızda ikili antlaşma olan devletlerin sayısı gittikçe artmaktadır. Mevcut durumda Amerika Birleşik Devletleri, Çin, Fas, Hindistan, Irak, İran, Kazakistan, Kırgızistan, Kuveyt, K.K.T.C., Lübnan, Mısır, Moğolistan, Özbekistan, Pakistan, Suriye, Tacikistan, Tunus,Türkmenistan ve Ürdün'le aramızda ceza istinabe konusunda ikili antlaşmalar bulunmaktadır.

Mütekabiliyet

Aramızda herhangi bir akdi bağ olmayan devletlerle yapılan adlî yardımlaşma işlemleri (Türkmenistan, Kanada, Kosova vb.) mütekabiliyet (karşılıklılık) prensibine göre yerine getirilir.

6.3. Uluslararası Ceza İstinabenin Temel Prensipleri

6.3.1. Talepler, Talep Edilen Devletin Mevzuatına Göre Yerine Getirilir

Adlî yardımlaşma talepleri, devleti mevzuatında öngörülen kurallara uygun olarak yerine getirilir. Ülkemizden giden talepler açısından düşünüldüğünde, eğer talebimiz o ülkenin mevzuatına uygun şekilde yerine getirilmişse, bizim mevzuatımıza göre de geçerli sayılır. Bu durum şöyle bir örnekle açıklanabilir:Amerika Birleşik Devletleri'nde FBI adlî kolluk görevi yapmaktadır. ABD mevzuatı gereğince talebin mahkeme veya savcılık tarafından yapılması fark etmeksizin FBI tarafından yerine getirilmektedir. Bu nedenle FBI'ın mahkeme talebi doğrultusunda aldığı sanık savunması hukukumuz açısından geçerli kabul edilmektedir.

6.3.2. Kural Olarak Masraf Alınmaz

Adlî yardımlaşma işlemleri kural olarak herhangi bir masraf alınmadan yerine getirilmektedir. Ancak doktor raporu, DNA analiz raporu, veya bilirkişi raporu gibi uzmanlık veya masraf gerektiren talepler için masraf talep edilebilir.

6.3.3. Evrak, Talep Edilen Devletin Resmî Diline Tercüme Edilir

İstisnaları olmakla birlikte adlî yardımlaşma evrakı talep edilen devletin resmi diline tercüme edilir. Evrak asıl nüshası ve tercümesiyle birlikte talep edilen devlete gönderilir.

6.4. Adlî Yardımlaşma Talebinin Reddi Sebepleri

CİKAYAS'ın 2. maddesine göre kendisinden yardım talep edilen taraf, aşağıdaki nedenlerle talebi reddedebilir:

6.4.1. Talep Edilen Devlet, Talebi Siyasî Suçlarla Veya Malî Suçlarla Ilgili Sayıyorsa

Siyasal suç kavramı konusunda tüm devletlerin üzerinde uzlaştığı bir tanım yoktur. Her devlet kendi tehlike algılamasına ve siyasi pozisyonuna göre siyasi suç tanımı yapmaktadır. Bunun sonucu olarak da bir devlet tarafından terör suçu olarak kabul edilen bir suç, bir başka devlet tarafından siyasi suç olarak kabul edilebilmekte; adlî yardımlaşma talebi bu gerekçe ile reddedilebilmektedir. Tanınmış bir terör uzmanı *"Terörizm de aynen güzellik gibi bakan kişiye göre değişmektedir."*demiştir.

CİKAYAS'ta mali suçlarla ilgili taleplerin yerine getirilmeyebileceği belirtilmişse de EK 1 nolu protokolde, bir talebin mali bir suça ilişkin olması nedeniyle reddedilemeyeceği belirtilmiştir. Ek 1 nolu protokol ülkemiz tarafından da onaylanıp yürürlüğe konulduğundan anılan protokole taraf olan diğer devletlerle mali suçlar konusunda da adlî yardımlaşma yapılması mümkündür.

6.4.2. İstenilen Devlet Talebin Yerine Getirilmesini Egemenlik, Güvenlik, Kamu Düzeni veya Diğer Öz Çıkarlarına Aykırı Görüyorsa

Red nedeni olarak gösterilen ve uygulanan bu kavramlar somut ve sınırları belli kavramlar olmayıp ülkeden ülkeye değişebilmektedir.

6.4.3. Çifte Cezalandırılabilirlik Koşulu

Çifte cezalandırılabilirlik koşulu Adlî yardımlaşma talebine konu olan suçun hem isteyen devlet hem de istenilen devlet mevzuatına göre suç olması anlamına gelmektedir. CİKAYAS'ta arama ve tutuklamaya ilişkin hükümlerin yer aldığı 5. madde haricinde çifte cezalandırılabilirlik koşuluna ilişkin bir düzenleme bulunmamaktadır. Buna rağmen taraf devletler kendi mevzuatına göre suç olmayan bir fiile ilişkin talepleri kamu düzenine aykırı olduğu gerekçesiyle yerine getirmemektedir.
Diğer yandan tarafı olduğumuz ikili Antlaşmaların çoğunda çifte cezalandırılabilirlik koşulu yer almaktadır. Örneğin Türkiye ile ABD arasındaki 1981 tarihli suçlu iadesi ve adlî yardımlaşma Antlaşmasının 22. maddesinde; talep edilen devletin kendi mevzuatında suç olmayan fiillere ilişkin talepleri reddedebileceği belirtilmiştir.

6.5. Siber Suçlar Avrupa Sözleşmesi

Siber Suçlar Avrupa Sözleşmesi'ni; Amerika Birleşik Devletleri, İngiltere, Fransa, Almanya, Japonya'nın da dâhil olduğu 10 devlet imzalamış ve ulusal parlamentosunda onaylayarak yürürlüğe koymuştur. Türkiye'nin de arasında olduğu 37 ülke Sözleşmeyi imzalamış ancak henüz parlamentosundan geçirmemiştir. Sözleşme 2012 yılı Aralık ayında onay için TBMM'ye gönderilmiş, Meclis Dışişleri Komisyonunda kabul edilerek Genel Kurula sevkedilmiştir. Halen (Ağustos 2013 tarihi itibariyle) Genel Kurul gündemine alınması beklenmektedir.

Sözleşme siber suçlar alanındaki adlî yardımlaşma konusunda kapsamlı

hükümler içermekte olup önemine binaen bu hükümler ve getirdiği yeniliklere aşağıda kısaca değinilmiştir.

Madde 23 - Adlî Yardımlaşma

Sözleşmenin 23. maddesi, taraf devletlere bilgisayar sistemlerine veya verilerine ilişkin ceza soruşturma veya kovuşturmalarında işbirliği yapma yükümlülüğü getirmektedir.

Madde 25 - Adlî Yardımlaşmaya Ilişkin Genel İlkeler

Sözleşmenin 25. maddesinde; taleplerin öncelikle talep edilen tarafın mevzuatına göre yerine getirileceği, talep edilen tarafın Sözleşmenin 2 ila 11. maddeleri arasında sayılan suçların kendi mevzuatı gereğince salt mali suç olması nedeniyle adlî yardımlaşma talebini reddedemeyeceği belirtilmiştir.

Madde 26 - Anında Iletilen Bilgiler

Sözleşmenin 26. maddesi ile taraf devletlerin adlî makamlarının kendi yürüttükleri soruşturmalar sırasında elde ettikleri bilgilerin diğer bir devlette bu sözleşme gereğince soruşturma başlatmaya yarayacağının anlaşılması hâlinde bu bilgileri doğrudan o devlete iletebileceği belirtilmiştir.

Madde 27 - Uluslararası Anlaşmaların Yürürlükte Bulunmadığı Durumlarda Gelen Adlî Yardımlaşma Taleplerine Ilişkin Usuller

Sözleşmenin 27. maddesinde taraflar arasında bir adlî yardımlaşma anlaşması bulunup bulunmamasına göre ikili ayrıma gidilmiştir.

Böyle bir anlaşma olmaması durumunda taraflar arasında bu maddenin 2 ila 10. paragrafları arasında yer alan adlî yardımlaşmaya ait usul hükümlerinin geçerli olacağı belirtilmiştir. Taraflar arasında bir adlî yardımlaşma antlaşması olması halinde ise 27. maddede yer alan usul hükümlerinin taraflar arasında geçerli olabilmesi için bunu açıkça kabul etmeleri gerekmektedir. Örneğin Türkiye ile ABD arasında karşılıklı adlî yardımlaşma antlaşması vardır. Buna rağmen (Türkiye bu sözleşmeyi imzaladığında) iki taraf bu konuda mutabakata varırsa siber suçlar alanındaki adlî yardımlaşma usulünde söz konusu ikili antlaşma hükümleri yerine bu sözleşmenin 27. maddesinde yer alan hükümlerin geçerli olması kararlaştırılabilir.

27. maddenin 2 ila 10. paragraflarında; talebe konu olan suçun talep edilen tarafça siyasi suç veya kamu düzenine veya egemenliğine aykırı görülmesi durumunda anılan tarafın talebi reddedilebileceği hükümleri yer almaktadır.

Diğer yandan, anılan paragraflarda ayrıca acil durumlarda tarafların adlî makamlarının doğrudan yazışabilecekleri böyle bir durumda talebin bir nüshasının ayrıca yetkili merkezi makama iletilmesi gerektiği, taleplerin veya sair yazışmaların İnterpol aracılığı ile de gönderilip alınabileceği belirtilmiştir.

Madde 29 - Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması

Sözleşmenin 29. maddesindetaraflardan biri, diğer tarafın ülkesinde yer alan bilgisayar verileri ile ilgili olarak adlî yardımlaşma talebinde bulunmayı planlıyorsa anılan taraftan söz konusu verilerin muhafaza edilmesini isteyebileceği belirtilmiştir.

Madde 30 - Korunan Trafik Verilerinin Açıklanması Işleminin Kolaylaştırılması

Sözleşmenin 30. maddesine göre29. madde gereğince kayıt muhafaza talebi yapıldığında talep edilen devlet eğer talep konusu verilerle ilgili olarak başka bir ülkede yer alan bir hizmet sağlayıcının da dahli olduğunu tespit ederse o hizmet sağlayıcının ve verilerin aktarıldığı yolun belirlenmesi için trafik verilerini açıklamalıdır. Yani talep edilen devlet trafik verilerini talep eden devlete vererek onun üçüncü devletteki verilere erişmesini kolaylaştırmalıdır.

Madde 31 - Saklanan Bilgisayar Verilerine Erişilmesine Ilişkin Adlî Yardımlaşma

Sözleşmenin 31. maddesi ile taraf devletlere diğer devletin ulusal sınırları içinde bulunan bilgisayar sisteminde yer alan veya depolanan verileri talep etme hakkı tanınmaktadır.

Madde 32 - Saklanan Bilgisayar Verilerine Izinli Şekilde ya da Bu Verilerin Halka Açık Olduğu Durumlarda Sınır Ötesinden Erişim Sağlamak

Sözleşmenin 32. maddesi ile taraf devletlere birbirlerinden izin almaksızın birbirlerinin ulusal sınırları içindeki açık bilgisayar verilerine erişimi, saklı bilgisayar verilerine ise bilgisayar sistemi üzerinden açıklama yetkisi olan kişinin iznini aldıktan sonra erişebilmesi veya bu bilgileri alabilmesi imkânı getirilmiştir.

Madde 33 - Trafik Verilerinin Gerçek Zamanlı Olarak Toplanması Konusunda Yardımlaşma

Sözleşmenin 33. maddesinde ulusal yasaları uygulanmak kaydıyla tarafların trafik verilerinin gerçek zamanlı olarak toplanması için birbirlerine yardımcı olacakları belirtilmiştir.

Madde 34 - İçerikle Ilgili Verilere Müdahale Edilmesi Konusunda Yardımlaşma

Sözleşmenin 33. maddesindetarafların ulusal yasaları uygulanmak kaydıyla özel iletişimlere ilişkin içerik bilgilerinin gerçek zamanlı olarak toplanması için birbirlerine yardımcı olacakları belirtilmiştir.

6.6. Siber Suçlarda Trafik Bilgisi / IP Numarası Teminine Yönelik Adlî Yardımlaşma Talepleri

Siber suçlarda şüpheliye ulaşmak için en yaygın şekilde kullanılan yöntem suça konu işlem yapılırken kullanılan IP numarası tespit edilerek, IP numarasının tahsis edildiği internet abonesini belirlemektir. Bu tür suçlarla ilgili olarak yapılan uluslararası adlî yardımlaşma taleplerinin büyük çoğunluğu da IP numarası veya trafik verisinin ilgili firmadan temin edilmesi talebini içermektedir.

Tespit edilen IP numarasını kullanan abonenin adresi internet kafe, otel veya alışveriş merkezi gibi yerler çıktığında şüphelinin tespiti oldukça zordur. Çünkü müşterilerine şifreli veya şifresiz şekilde kablosuz internet hizmeti sağlayan bu tür yerlerde hangi kullanıcının internete girdiğine ilişkin kayıt tutulmamaktadır. Tespit edilen adres konut çıktığında ise uygulamada konutta yaşayanların ifadesine başvurulmaktadır. Ancak böyle bir durumda kişinin suçu ikrar etmemesi durumunda suçun ispatı için soruşturmanın derinleştirilmesi gerekmektedir. Ayrıca wifi kullanıldığı için 3. kişilerin de o IP'den internete girebildiği veya bir dönem konutta misafir olarak başkalarının da kaldığı yönündeki savunmalar sübut sorununu biraz daha derinleştirmektedir.

Diğer yandan IP numarası kullanılarak tespit edilen adreste sadece internet abonesi yaşasa dahi o kişi ikrarda bulunmadıkça veya diğer delillerle desteklenmedikçe sadece IP numarası esas alınarak o kişi hakkında mahkûmiyet hükmü kurulamamaktadır. Suçun kesin şekilde ispatlanabilmesi için adreste arama yapılması, bilgisayar veya bilgisayar özelliği taşıyan tablet, akıllı telefon ve hatta smart tv gibi cihazlar tespit edilip CMK'nın 134. maddesi gereğince bu cihazlarda içerik araması yapılması gerekmektedir. Cihazlar formatlanmışsa veya özel programlar kullanılarak içerik silinmişse aranılan içeriğe ulaşma şansı azalmaktadır. Ayrıca CMK'nın 134. maddesine göre arama yapılırken suç ile uygulanacak tedbir arasındaki dengenin gözetilmesi gerekmektedir.

6.7. Siber Suçlarda Suçun İşlendiği Yerin veya Şüphelinin Bulunduğu Yerin Bilinmemesinden Kaynaklanan Sorunlar :

Türk Ceza Kanunu'nun 11. ve 12. maddesi gereğince yurt dışında işlenen suçlarla ilgili olarak Türkiye'de kovuşturma yapılabilmesi için; (diğer şartların yanında) şüphelinin Türkiye'de bulunması ve suç için kanunda öngörülen cezanın alt sınırının 1 yıl veya üzerinde olması şartları birlikte mevcut olmalıdır.

Ancak yabancı bir devletten IP bilgilerinin veya trafik kayıtlarının temine ilişkin Adlî yardımlaşma talebinde bulunurken çoğu zaman başlangıçta suçun Türkiye içinde mi dışında mı işlendiği belli değildir. Adlî yardımlaşma sonucu elde edilen bilgilerden şüphelinin yurtdışında olduğu anlaşılıyorsa kovuşturma aşamasına geçilme imkânı bulunmamakta bu da sonuca ulaşmayacak bir soruşturma için adlî yardımlaşma talebinde bulunmuş olmak anlamına gelmektedir.

6.8. Adlî Makamlarca Doğrudan IP Bilgisi Trafik Verisi Temin Edilebilecek Durumlar:

Facebook, Twitter vb. yer sağlayıcı firmalar kural olarak adlî makamların kendilerinden talep ettikleri IP bilgisi, trafik verisi veya içeriğe ilişkin bilgileri vermemekte bunun adlî yardımlaşma yoluyla firma merkezinin bulunduğu devlet yapılacak bir taleple elde edilebileceğini belirtmektedirler.

Bu kuralın istisnalarından biri;Hotmail, Windoswslive, MSN gibi Microsoft firmasına ait bütün internet firmalarının soruşturma veya kovuşturma aşamasından adlî makamlarımız tarafından doğrudan Türkiye'deki temsilciliğine başvurulduğunda IP bilgilerini ve diğer trafik bilgilerini vermesidir. Fakat içeriğin tespitine ilişkin taleplerin ABD adlî makamlarına gönderilecek adlî yardımlaşma talebi yoluyla istenmesi gerektiğini belirtmektedirler.

Buna diğer bir istisna olarak da Facebook'un belli şartlarda IP veya trafik bilgisini doğrudan vermesi gösterilebilir. Facebook; intihara teşebbüs, öldürmeye teşebbüs, kayıp bir şahsın bulunması veya çocukların cinsel istismarı suçlarını acil husus kabul ederek soruşturma makamlarımız tarafından doğrudan talepte bulunulduğunda IP veya trafik bilgilerini vermektedir.

6.9. Siber Suçlarda 7/24 Kapsamında Uluslararası İstinabe

Siber Suçlar Avrupa Sözleşmesi'nin 35. maddesinde taraf devletlerden her birine 7 gün 24 saat hizmet verebilen irtibat noktalarının kurulması yükümlülüğü getirilmiştir.

35. maddenin 4. fıkrasında ise irtibat noktalarının adlî yardımlaşma ve iadede sorumlu merciiler olması veya onların bir parçası durumunda olması gerektiği belirtildikten sonra eğer anılan durum yoksa irtibat noktasının bahsi geçen mercilerle hızlı şekilde koordinasyon sağlayacak durumda olması gerektiği belirtilmiştir.

Türkiye için 7/24 irtibat noktasının Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı olması yönünde Sözleşmeye beyanda bulunulması kararlaştırılmıştır. Ancak adlî yardımlaşma konusunda merkezi makam olan Adalet Bakanlığı Uluslar arası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nün de anılan Başkanlık ile birlikte 7/24 irtibat noktası olması yönünde girişimler bulunmaktadır.

6.10. Siber Suçlarda Bazı Ülkelerle Adlî Yardımlaşma

6.10.1. Amerika Birleşik Devletleri

Facebook, Google, Yahoo, Twitter, Skype, Youtube, Hotmail, M. Messenger gibi internet dünyasının en çok kullanılan yer sağlayıcı firmalarının merkezi Amerika Birleşik Devletleri'nde bulunmaktadır. İnternet ortamında işlenen suçların büyük çoğunluğu da bu yer sağlayıcı firmalar üzerinden işlenmektedir. İstisnalar dışında bu firmalar suç soruşturması nedeniyle talep edilen IP veya benzeri bilgileri doğrudan adlî mercilerle paylaşmamakta, bunun ancak ABD'ye yapılacak uluslararası adlî yardımlaşma talebi ile mümkün olabileceğini belirtmektedirler.

Soruşturma konusu suç, anılan firmaların başka bir ülkede yer alan şubesi, temsilciliği veya reklam işlerini idare için kurulmuş yan kuruluşu üzerinden işlenmiş olsa dahi IP numarası veya diğer trafik bilgileri firmaların ABD'deki merkezlerinde tutulduğundan diğer ülkelere yapılan adlî yardımlaşma talepleri yerine getirilememektedir.

Diğer yandan Amerika Birleşik Devletleri'nin adlî yardımlaşma uygulaması suç türlerine göre değişebildiğinden aşağıda bu konuda bazı bilgilere yer verilmiştir:

6.10.2. Hakaret Suçu

Amerika Birleşik Devletleri'nin ceza mevzuatında hakaret veya sövme suçlarına ilişkin bir düzenleme bulunmamaktadır. Bu tür suçlara ilişkin olarak yapılan IP kaydı temini, ifade alınması, adres tespiti vb. bütün adlî yardımlaşma talepleri ABD makamları tarafından 'Bu tür eylemlerin ABD Anayasası tarafından korunan ifade

özgürlüğü kapsamında olduğu, ceza davasına değil ancak belli şartlarda tazminata konu olabileceği' belirtilerek işlemsiz iade edilmektedir. Bu nedenle hakaret suçuna ilişkin adlî yardımlaşma talepleri Türkiye merkezi makamı tarafından ABD'ye gönderilmeyip adlî makama iade edilmektedir.

ABD merkezi makamı ret gerekçesi olarak Türkiye ile ABD arasındaki adlî yardımlaşmaya ilişkin 1981 tarihli antlaşmanın 22. maddesini göstermektedir. 22. madde, taraf devletlerin her birine kendisinde suç olmayan eylemlere ilişkin talepleri yerine getirmeme yetkisi vermektedir. Diğer yandan anılan ülke Federal Yüksek Mahkemesi tarafından ifade özgürlüğü çok geniş yorumlanmaktadır. Bu kapsamda devlet başkanlarını, kamu görevlilerini veya dinen kutsal sayılan değerleri hedef alan hakaret veya aşağılama eylemleri dahi suç sayılmamaktadır.

6.10.3. İftira Suçu

Adlî makamlarımızca suç açıkça hakaret olarak nitelendirilmeyip 'iftira' olarak nitelendirilse de (TCK'nın 267. maddesindeki şartlar dışında) bir kişi hakkında yazılı, sözlü veya görüntülü olarak sarfedilen rahatsız edici beyanlar da ABD makamları tarafından ifade özgürlüğü kapsamında değerlendirilmektedir.
Örneğin internet ortamında, bir memurun rüşvet aldığı şeklinde bir haber yapılmışsa, ABD makamları bu eylemi ifade özgürlüğü olarak değerlendirmektedirler.

Ancak anılan uydurma haberde yer, zaman, mekân kişi adları da belirtilerek suçun unsurları uydurulmuşsa ve bu isnatlar nedeniyle memur hakkında rüşvet almak suçundan soruşturma başlatılmışsa ve sonraki aşamada memurun böyle bir suçu işlemediği bilinmesine rağmen kasıtlı olarak haber yapıldığı anlaşılıp şüpheli hakkında TCK'nın 267. maddesi gereğince soruşturma başlatılmışsa bu durumun ABD makamları tarafından ifade özgürlüğü dışında değerlendirileceği düşünülmektedir. Ancak bu durumda şüphelinin gerçeği bilmesine rağmen suça konu iddiaları kasıtlı olarak yaptığına ilişkin kanaat sağlayacak bulguların dosyada gösterilmesi gerekmektedir.

6.10.4. Hakaret Suçunun Yanında İşlenen Diğer Suçlar

Adlî yardımlaşma talebi, hakaret suçunun yanında başka suçları da (örneğin tehdit, yaralama gibi) içerse dahi ABD adlî makamları tarafından ikili Antlaşmanın 22. maddesi gerekçe gösterilerek talep yerine getirilmemektedir. Bu nedenle hakaret suçunun yanında diğer suçların da olduğu soruşturmalara ilişkin adlî yardımlaşma taleplerinde hakaret suçu talebe konu edilmeksizin diğer suçlar üzerinden talepte bulunulduğunda talep yerine getirilebilmektedir. Örneğin kasten yaralama ve tehdit suçlarından yürütülen bir soruşturmada müşteki ifadesinin alınması istemiyle hazırlanacak bir talepname sadece kasten yaralama suçu esas alınarak hazırlanmalıdır. Bu durumda talepname içeriğinde veya eklerinde hakaret suçuna ilişkin talep veya bilgilere yer verilmemesi gerekmektedir.

Kovuşturma aşamasında yapılan adlî yardımlaşma taleplerinde iddianamenin talepnameye eklenmesi zorunludur. Ancak, bu durumda da eklenen iddianamede hakaret suçuna ilişkin bilgiler yer alacağından talep yerine getirilmemektedir. Bu nedenle kovuşturma aşamasına geçilmişse ve iddianamede hakaret suçuna ilişkin bilgiler de yer alıyorsa adlî yardımlaşma talebinin yerine getirilme imkânı bulunmamaktadır.

6.10.5. Banka Veya Kredi Kartı Bilgileri Kullanılarak Internet Ortamında İşlenen Suçlar

ABD uygulamasında savcı zarar azlığı vb. unsurları dikkate alarak soruşturma açılmasında kamu yararı bulunmadığını belirterek herhangi bir suçu soruşturmama yetkisine sahiptir. İç hukukta yer alan bu uygulamayı da dikkate alarak ABD makamları diğer ülkelerden gelen talepleri öncelik sırasına koymakta, yoğun iş yükü ve kaynak yetersizliği nedeniyle düşük öncelikli gördükleri suçlara ilişkin talepleri yerine getirmemektedir.

Bu kapsamda; hukuka aykırı şekilde ele geçirilen kredi kartı veya banka hesap bilgilerini kullanarak internet üzerinden harcama yapılması, başkasının hesabına para aktarılması gibi suçlara ilişkin ceza istinabe talepleri ABD merkezi makamınca yerine getirilmemektedir. Buna gerekçe olarak da bu tür suçlarda banka tarafından mağdurların zararının karşılandığından mağdurun zararının kalmaması ve bu tür suçların ABD uygulamasında düşük öncelikli sayılması gösterilmektedir. Ancak bir örgüt kapsamında veya organize şekilde veya çok sayıda kişiye yönelik olarak işlenme ve büyük zararlara neden olma gibi suçu ağırlaştırıcı unsurlar varsa bunu gösterir ilave bilgi ve belgeler iletildiğinde talebin yeniden değerlendirileceği belirtilmektedir.

6.10.6. Özel Hayatın Gizliliğini Ihlal Suçu Ile Ilgili Adlî Yardımlaşma

Mağdurun fotoğrafı bir şekilde ele geçirilerek onun adına sahte facebook vb. sosyal paylaşım hesabı açılması ve kullanılması veya mağdurun ismi veya bilgileri kullanılarak açılan sosyal paylaşım hesaplarında mağdurla ilgisi olmayan 3. kişilerin uygunsuz fotoğraflarının kullanılması veya çeşitli yazılar yazılmasına ilişkin taleplerde ABD adlî makamları, fotoğrafın mağdurdan çalındığına veya hukuka aykırı şekilde ele geçirildiğine ilişkin delil bulunmadığı, mağdurun internet ortamında bir şekilde yer alan fotoğrafını kullanarak gerçekleştirilen bu tür fiillerin veya yukarıda sayılan diğer fiillerin ABD mevzuatında ceza davasına konu olmadığı, yalnızca hukukî ihtilaf olarak kabul edilebileceğini belirterek adlî yardımlaşma taleplerini reddetmektedir.

6.10.7. Oyun Siteleri veya Karakterleri Ile Ilgili Talepler

Kullanıcılar tarafından oluşturulan bazı oyun karakterlerinin şifre kırılarak veya başka bir şekilde şüpheli tarafından ele geçirilmesi eyleminin suç oluşturduğu belirtilerek yapılan adlî yardımlaşma taleplerinde;

- Söz konusu oyun sitesi üzerinde mağdur tarafından oluşturulan ve suça konu olan kullanıcı hesabının /profilinin bir bilişim sistemi olup olmadığı, bilişim sistemi ise hangi özellikleri nedeniyle bilişim sistemi kabul edildiği açıklanmalıdır.

- Çalındığı iddia edilen 'oyun malzemesi / karakteri' kavramının ne anlama geldiği, hukuken korunması gereken bir varlığa sahip olup olmadığı, hukuken korunması gereken bir varlığa sahipse hangi özelliği nedeniyle hukuken korunduğu, maddî değeri varsa ne kadar olduğu, bu değerin nasıl tespit edildiği açıklanmalıdır.

6.11. Siber Suçlarda Adlî Yardımlaşma Evrakının Hazırlanması

Adlî yardımlaşma evrakı, talepname ve eklerinden oluşmaktadır. Siber suçlara ilişkin adlî yardımlaşma talebinde bulunulurken hazırlanan talepname ve ekinde yer

alması gereken bilgi ve belgeler diğer suçlar için hazırlanan evraktan farklı yönlere sahiptir. Bu bölümde genel hatlarıyla buna ilişkin bilgilere yer verilecektir.

6.11.1. Adlî Yardımlaşma Talepnamesi

Adlî yardımlaşma talepnamesi talep eden adlî makam tarafından talep edilen ülke adlî makamına hitaben düzenlenen özel bir mektup türü olarak tanımlanabilir.

Talepname metninde;

Talepte bulunan adlî makamın adı, suç tarihi, suçun tanımına, ilgili suçun işleniş şekline ilişkin açıklamalara, ceza hükümlerinin numaralarına, dinlenecek kişinin isim ve adresine, talebin dayanağı olan uluslararası antlaşmanın ismine yer verilmelidir.

Talepname ekinde;

İddianameye (kovuşturma aşamasında), uygulanması muhtemel kanun maddelerinin metinlerine, şikayet, savunma veya tanık ifade suretlerine, delil niteliğindeki belgelere, talepnamenin ve ekli evrakın tercümesine yer verilmelidir.

6.11.2. İnternet Ortamında Işlenen Suçlara Ilişkin Adlî Yardımlaşma Talebinde Bulunurken Suçun Konusuna Göre Ayrıca Aşağıdaki Hususlar Önem Taşımaktadır

- Suça konu içeriğin sosyal paylaşım hesabına veya web sayfasında konulma ve kaldırılma tarihleri talepnamede belirtilmelidir.

- Suça konu içerik bir e-posta adresinden gönderilmişse gönderen ve alan e-posta adresleri ile gönderilme tarihi talepnamede gösterilmelidir.

-Yayınlanan yazı veya görüntünün, gönderilen e-postanın veya sosyal paylaşım sitelerinde oluşturulan kullanıcı hesapları üzerinde gerçekleştirilen eylemlerin hangi nitelikleri nedeniyle suç oluşturduğu talepnamede detaylı şekilde açıklanmalıdır.

- Talebe konu suçun tanımı yapılarak, somut olayda suçun unsurlarının ne şekilde oluştuğu hususu talepname metninde irdelenmelidir.

-Suçun konusu bir video görüntüsü ise talepname metninde mümkün olduğu ölçüde detaylandırarak video içeriği hakkında bilgi verilmeli, videonun yer aldığı link talepnamede belirtilmeli ve yine mümkünse içerik bir CD'ye kaydedilerek talepnameye eklenmelidir.

-Suçun konusuna göre; web sayfasının veya gönderilen e-mailin okunaklı şekilde çıktısı alınmalıdır. Suça konu sayfaya erişim sağlanamıyorsa veya suça konu içerik değiştirilmişse bu durum bir tutanağa bağlanarak talepnameye eklenmelidir.

6.11.3. Facebook Üzerinden Işlenen Suçlarla Ilgili Taleplerde Talepname Hazırlanırken Aşağıdaki Hususlar Dikkate Alınmalıdır

-Şüphelinin kullanıcı adı /profil bilgisi veya facebook'a kayıt olurken kullandığı

e-posta adresinin tam adı talepnamede belirtilmelidir. Bu iki bilgiden herhangi birinin talepnamede olması yeterlidir. Ancak bu bilgilerden hiç biri talepnamede belirtilmemişse trafik verisi tespiti, IP kaydı tespiti veya içerik tespitine ilişkin talepler yerine getirilememektedir.

-Talepnamede olması gereken kullanıcı adı veya profil bilgisi şüphelinin facebook duvarındaki ismi değildir. Örneğin talepnamede 'KASIRGA' şeklindeki nick name veya 'Işın Kılıcı' şeklindeki isim soy isimden oluşan profil adının yazılması durumunda talep yerine getirilememektedir. Çünkü aynı adı veya nick name'i kullanan başka kişiler de olabilmektedir.

-Talepnamede olması gereken kullanıcı adı; suça konu facebook sayfası açıldığında görev çubuğu bölümünde yer alan bilgilerin tamamıdır. Bu bilgilerin tamemen kopyalanarak talepname içeriğine yazılması gerekmektedir.

Örnek : https://www.facebook.com/profile.php?id=1613577911

-Eğer kullanıcı adı tespit edilemiyorsa şüphelinin facebook'a kayıt olurken kullandığı e-posta adresinin belirtilmesi gerekmektedir.

Örnek : kaya.toprak@gmail.com

6.12. Suça Konu İçeriğin Yayından Kaldırılması

Bütün sosyal paylaşım sitelerinde sakıncalı içeriğin kaldırılması için kullanıcılar tarafından bildirimde bulunmaya imkân verecek ekran bölümleri bulunmaktadır. Kullanıcılar tarafından yapılan şikayetler büyük oranda dikkate alınarak içerik kaldırılmaktadır.

Ancak büyük çoğunluğu ABD merkezli olan bu siteler genel olarak ifade özgürlüğünü geniş şekilde yorumlamakta, mevzuatımıza göre hakaret sayılabilecek bazı söylemleri (özellikle de politikacılar aleyhindekileri) eleştiri sınırları içinde kabul ederek içeriği kaldırma taleplerini reddedebilmektedir.

6.13. Trafik Verisi veya İçerik Muhafaza Talebi

Siber Suçlar Avrupa Sözleşmesi, taraf devletlere IP bilgisinin de içinde bulunduğu trafik verilerini belli bir süre saklama konusunda gerekli yasal alt yapıyı oluşturma yükümlülüğü getirmiştir. Sözleşmeye taraf olsun olmasın çeşitli devletlerin mevzuatlarında yer alan bu süreler farklılık gösterebilmektedir. Ayrıca yer sağlayıcı firmaların uygulamaları farklılık göstermekle birlikte firmaların çoğu kanuni süre dolduktan sonra kendilerine iletilen talepleri kaydın silindiğini belirterek reddedebilmektedirler.

Bu nedenle uluslararası adlî yardımlaşma yoluyla trafik bilgisi talebinde bulunulacaksa bu talep muhatap devletin mevzuatında düzenlenen kayıt muhafaza süresi içinde ilgili firmalara gönderilmelidir.

Türkiye'de ise 5651 Sayılı Kanun'da erişim sağlayıcının (servis sağlayıcının) yükümlülüklerini düzenleyen 6. maddenin 1. fıkrasına göre erişim sağlayıcı trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek

süre kadar saklamakla yükümlüdür. 5651 Sayılı Kanuna dayanarak hazırlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin 8 / b maddesine göre erişim sağlayıcı trafik bilgisini 1 yıl saklamakla yükümlüdür.

Telekomünikasyon İletişim Başkanlığı'nda kural olarak trafik bilgisi tutulmamaktadır. Ancak uygulamada TİB adlî makamlardan gelen trafik bilgisi temin talebi üzerine ilgili erişim sağlayıcıdan bu bilgileri temin edip adlî makama iletebilmektedir. TİB, bu şekilde temin ettiği trafik bilgilerini dava zamanaşımı süresinin sonuna kadar muhafaza etmektedir.

ABD mevzuatında trafik bilgilerinin*(IP kayıtları vb.) saklanma süresi :

ABD mevzuatına göre (18 U.S.C. § 2703 - f) internet ortamında işlenen suçlara ilişkin trafik bilgileri yer sağlayıcılar veya erişim sağlayıcılar tarafından 90 gün süreyle saklanmaktadır. Bu süre içinde resmi otoritelerce başvurulduğunda anılan saklama süresine 90 gün daha ilave edilmektedir.

7

ULUSLARARASI İŞ BİRLİĞİNE İLİŞKİN ÖRNEK MATERYALLER

facebook'tan IP kaydı, bilgi-belge temini için
talepname örneği

Türkiye Cumhuriyeti / /
Cumhuriyet Başsavcılığı

Amerika Birleşik Devletleri Yetkili Adli Makamına

Talebin konusu :

Örn. Suç işlenirken kullanılan IP kayıtlarının ve bu kayıtları kullanan şüpheliye ait bilgilerin temini

Soruşturma numarası :

Örn : 2012 / 41975

Suça İlişkin Bilgiler :

Suç Tarihi :
Suçun tanımı : *Örn. Tehdit*
İlgili Ceza Hükümleri : *Örn. 5237 Sayılı Türk Ceza Kanunu, Madde 106*

Soruşturmanın tarafları :

Şüpheli : *Örn. Şerif ŞER, Turabi oğlu 1982 doğumlu*
(veya bilinmiyorsa) şüpheli henüz tespit edilememiştir
Müşteki : *Örn. Taylan TAY, Behlül oğlu 1980 doğumlu*

Facebook hesabına ilişkin bilgiler :

***Müştekinin facebook ID numarası ve kullanıcı adı :** *Örn. Kullanıcı adı : Şerif*
ID no : https://www.facebook.com/profile.php?id=1613577911
(Müştekinin ID numarasının yazılması aşağıdaki durumlarda zorunludur)

1- *şüpheli suçu müştekinin facebook hesabını kullanarak işlemişse, örn : müştekinin şifresini kırıp onun facebook duvarına şiddet içeren bir söz yazmışsa veya*

2- *şüpheli kendi hesabından veya başka bir facebook hesabından müştekiye tehdit içeren mesajlar göndermişse ve gönderen hesabın ID numarası bilinmiyorsa)*

***Şüphelinin facebook ID numarası ve kullanıcı adı :** *(aşağıdaki durumlarda yazılması zorunludur)*

1- *şüpheli kendi hesabını kullanarak suç işlemişse örn : şüpheli kendi hesabının duvarına yazdığı bir yazı ile müştekiyi tehdit etmişse veya kendi sayfasına gösterimi suç olan bir içerik koymuşsa,*

2- *şüpheli kendi hesabından veya başka bir facebook hesabından müştekiye tehdit içeren mesajlar göndermişse*

***Şüphelinin facebook hesabını oluştururken kullandığı e-mail adresi :**

Müşteki veya şüphelinin facebook hesabının ID numarası bilinmiyorsa aşağıdaki durumlar dikkate alınarak suçta kullanılan e-mail adresi talepnamede gösterilmelidir :

-şüphelinin suça konu mesajları gönderdiği facebook hesabını oluştururken kullandığı e-mail adresi veya

-şüpheli, müşteki ya da herhangi bir kişi adına sahte bir facebook hesabı oluşturup o hesapta yazı veya görüntü yayınlayarak suç işlemişse şüphelinin o hesabı oluştururken kullandığı e-mail adresi belirtilmelidir.

Önemli not : *yukarıda (*) işaretiyle başlayan bölümlerdeki bilgilerden en az bir tanesinin talepnamede yer alması zorunludur, bu bilgilerin yer almadığı talepler yerine getirilememektedir. Mevcut olması halinde birden fazlasının (örn hem sanığın hem de müştekinin ID numarası gibi) yazılması, talebin yerine getirilmesini çabuklaştıracaktır.*

Facebook ID no hakkında daha fazla bilgi almak için web sayfamızı ziyaret ediniz.

Suçun işlenişine ilişkin olgular :

Örn :

Kimliği tespit edilemeyen şüpheli, müşteki X'in Facebook hesabının şifresini onun izni dışında ele geçirmiştir. Şüpheli müştekinin Facebook duvarına .... tarihinde 'Eğer bir daha benden habersiz işler çevirirsen senin canına okurum' şeklinde tehdit içerikli bir söz yazmıştır. Müşteki, söz konusu yazıyı silmek için şifresiyle hesabına girmek istemiştir ancak şifre değiştiği için müşteki bunu yapamamıştır. Müştekinin Facebook şirketine şikayette bulunması üzerine .... tarihinde müştekinin facebook hesabı kapatılmıştır.

Suçun hukuki niteliği :

(suçun vasıflandırılması adli makamlarımızın takdirinde olup aşağıdaki suç nitelemeleri örnek olması amacıyla yazılmıştır.)

Şüpheli tarafından yazılan 'Eğer bir daha benden habersiz işler çevirirsen senin canına okurum' sözü müştekiye yönelik ciddi bir şiddet unsuru içerdiğinden bu eylem tehdit suçunu oluşturmaktadır. 'Canına okurum' tabiri 'ciddi şekilde zarar veririm', 'seni yaralarım' hatta 'seni öldürürüm' anlamlarına gelebilir. Bu sözün bu anlamlara geldiği toplum tarafından bilinmektedir.. Böyle bir tehdit sözü, normal koşullarda muhatabında korkuya neden olabilir ve onu tehdit eden kişinin isteği yönünde davranmaya zorlayabilir.

Talep edilen adli yardımlaşma :

Başsavcılığımız tarafından şüpheli hakkında yukarıda belirtilen suçlar nedeniyle soruşturma yapılmaktadır. Soruşturmanın tamamlanabilmesi için --- *(örn, soruşturmaya konu işleme ait IP bilgilerine)* ihtiyaç duyulmaktadır.

Adli yardımlaşma talebinin dayanağı :

Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Adli Yardımlaşma Antlaşması

Garantiler :

Bu talep ceza soruşturması / kovuşturması ile ilgilidir.

Elde edilecek bilgiler yasal sınırlar içinde kullanılacak ilgili kişilerin yasal hakları ihlal edilmeyecektir.

Bu talep; kişiler hakkında politik görüş, din,dil,ırk,cinsiyet,milliyet gibi konularda ayrımcılık yapılmasına ilişkin bir amaç içermez ve bu yönde sonuçlar doğuracak şekilde kullanılmaz.

Sonuç :

Yukarıda belirtilen adli yardım talebinin yerine getirilmesini rica eder ve bu vesileyle yardımlarınız için şimdiden teşekkür eder, en derin saygılarımı sunarım.

(isim, soyadı, sicil no.)

(Cumhuriyet Savcısı)

(İmza)

EKLER:

1) İfade suretleri (Mevcutsa)

2) Davaya konu facebook sayfasının çıktısı (okunaklı ve mümkünse renkli)

3) Bilirkişi raporu (mevcutsa)

4) Yargılamaya esas olan ceza hükümleri (usul hükümlerine gerek yok)

5) Yukarıda sayılı evrakın tercümeleri

Not :

1- Kollukla yapılan yazışmalar, tercümeye gönderme yazıları, sarf kararı gibi yabancı adli makamı ilgilendirmeyen evrak talepnameye eklenmemelidir.

2- Kolay incelenebilmesi için evrak delinerek telli dosyaya takılmalıdır. Evrakı tutturmak için zımba kullanılmamalıdır.

*3- Evrak 2 takım halinde düzenlenmeli ve delinerek telli dosyaya takılmalıdır. Evrakta zımba kullanılmamalıdır. Evrakın kolayca tasnifi ve arşivlenmesi için **her bir takımda** evrakın Türkçesi üstte, tercümesi altta olmalıdır.*

Dosya düzeni : Bakanlığa hitaplı üst yazı, 1. takım evrak (Türkçesi üstte / tercümesi altta), 2. takım evrak (Türkçesi üstte / tercümesi altta),

Kovuşturma aşaması bilgi belge temini

Türkiye Cumhuriyeti / /

Ceza Mahkemesi

--- Yetkili Adli Makamına

Talebin konusu :

Örn. Bilgi ve belge temini

Davanın Esas numarası :

Örn : 2012 / 41975

İddianameye ilişkin bilgiler :

İddianameyi düzenleyen Savcılık :

Tarih ve numarası :

Yargılama konusu suça ilişkin bilgiler :

Suç Tarihi :

Suçun tanımı : *Örn Dolandırıcılık*

İlgili Ceza Hükümleri : Örn. 5237 Sayılı Türk Ceza Kanunu Madde 158 , -- , --

Suçun işleniş şekli :

Yukarıda belirtilen iddianame ile sanık X hakkında Mahkememize kamu davası açılmıştır. Sanığın, üzerine atılı suçu / suçları aşağıdaki şekilde işlediği iddia edilmektedir :

Örnek olay :

Müşteki M'nin G. Bankasının Giresun Şubesinde yatırım hesabı bulunmaktadır. Müştekinin yurt dışında olduğu 12.08.2012 tarihinde anılan banka şubesine müşteki tarafından gönderildiği izlenimi verilen bir e-posta gönderilmiştir. E-posta'da 28.08.2012 tarihinde bir teminat yatırmak üzere 100.000 dolar nakit çekme talebi bulunmaktadır. Ertesi gün kendisini H ismiyle tanıtan sanık S bankayı arayarak kendisinin müştekinin avukatı olduğunu ve elindeki vekaletname gereğince söz konusu parayı çekeceğini belirtmiştir. Sanık S 16.08.2012

tarihinde banka şubesine gelerek sahte vekaletnameyi ibraz etmiştir. Olaydan şüphelenen banka sorumlusunun polise haber vermesi üzerine Sanık S yakalanmıştır. Sanık, e-postayı müştekinin gönderdiğini ve vekaletnamenin müşteki tarafından kendisine verildiğini ileri sürmüştür.

Talep edilen adli yardımlaşma :

Yargılamanın tamamlanabilmesi için lütfen aşağıdaki bilgi veya belgeleri Mahkememize gönderiniz :

1- 12.08.2012 tarihinde sgul@gmail.com hesabından gönderilen e-postanın gönderildiği bilgisayara ait IP kayıtları,
2- IP kayıtları ülkenize ait bir adresten gönderilmişse bu adrese ait bilgiler,

Adli yardımlaşma talebinin dayanağı :

Bu kısma isteme dayanak teşkil eden sözleşmenin adı yazılmalıdır.
Taraf olduğumuz çok taraflı ve ikili sözleşmelerin metinlerine ve listesine aşağıdaki linkten ulaşılabilir:
http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adlisbirligi_ceza/cz_istinabe.html

Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi için örnek :
Türkiye ve ……'nın birlikte taraf oldukları Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi (ETS 30)

İkili anlaşma için örnek :
(ABD) : Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Adli Yardımlaşma Antlaşması

Mütekabiliyet uygulamasına örnek:
(Kanada) : Türkiye Cumhuriyeti ile Kanada arasındaki adli yardımlaşma uygulamasına esas olan mütekabiliyet ilkesi

Garantiler :

Bu talep ceza soruşturması / kovuşturması ile ilgilidir.

Elde edilecek bilgiler yasal sınırlar içinde kullanılacak ilgili kişilerin yasal hakları ihlal edilmeyecektir.

Bu talep; kişiler hakkında politik görüş,din,dil,ırk,cinsiyet,milliyet gibi konularda ayrımcılık yapılmasına ilişkin bir amaç içermez ve bu yönde

Sonuç :

Yukarıda belirtilen adli yardım talebinin yerine getirilmesini rica eder ve bu vesileyle yardımlarınız için şimdiden teşekkür eder, en derin saygılarımı sunarım.

(isim, soyadı, sicil no.)
HAKİM
(İmza)

EKLER:

1) İddianame
2) Bilirkişi raporu (mevcutsa ve gerekli olduğu ölçüde)
3) İlgili ceza hükümleri
4) Yukarıda sayılı evrakın tercümeleri

Bilişim sistemine zarar verilmesi suçu
(TCK'nın 244. maddesi) talepname örneği
bilgi-temini

Türkiye Cumhuriyeti
Cumhuriyet Başsavcılığı

--- Yetkili Adli Makamına

Talebin konusu :

Örn. Suç işlenirken kullanılan IP kayıtlarının ve bu kayıtları kullanan şüpheliye ait bilgilerin temini
ve/ veya Şüpheli XY' nin savunmasının alınması
ve / veya Müşteki CK nin ifadesinin alınması

Soruşturma numarası :

Örn : 2012 / 41975

Soruşturmanın tarafları :

Şüpheli : *Örn. Şerif ŞER, Turabi oğlu 1982 doğumlu*
(veya bilinmiyorsa) şüpheli henüz tespit edilememiştir

Müşteki : *Örn. Taylan TAY, Behlül oğlu 1980 doğumlu*

Suça İlişkin Bilgiler :

Suçun tanımı : *Örn 1. Bilişim sistemini engelleme, bozma ,*

Suç Tarihi :

İlgili ceza hükümleri : *Örn. 5237 Sayılı Türk Ceza Kanunu; madde 244 (1. ve 3. fıkralar) madde 326, madde 53 (usul hükümlerini yazmaya gerek yoktur)*

Suçun işleniş şekli :

Açıklama: Tercümede meydana gelen kayıplar ve anlam kaymaları nedeniyle çok uzun veya devrik cümleler yabancı adli makamlar tarafından anlaşılamamaktadır. Özellikle iddianamelerden kopyalanarak talepnamelere eklenen paragraflarda yer alan sıralı cümle yapısı ve devrik cümleler tercüme sırasında anlam değişikliğine uğramaktadır. Bu nedenle kısa ve düz cümlelerin kullanıldığı bir anlatım tercih edilmeli, talepnamenin Türkçesinden çok tercümesinin alacağı şeklin önemli olduğu dikkate alınmalıdır.

Örnek olay :

Kimliği tespit edilemeyen şüpheliler; HAVIJ isimli bir program kullanarak .... Kurumuna ait www.---.gov.tr isimli resmi web sayfasını hedef alan siber saldırılar düzenlemişlerdir. HAVIJ programı internet sitelerinin bulunduğu serverler üzerindeki veri tabanlarını otomatik olarak tarayan ve SQL Injection açığı bularak veri tabanlarındaki bilgilere yetkisiz erişim sağlayan bir programdır.

Şüpheliler 12 Şubat 2011 tarihinde onlinekayıt@--.gov.tr isimli e-posta adresini ele geçirerek online --- başvurusu yapan kişilerin bilgilerinin yer aldığı veri tabanını ele geçirmişlerdir .
Şüpheliler HAVIJ programını kullanılarak 14 Ocak 2012 tarihinden itibaren .... Kurumu tarafından güvenli bilgilerin depolandığı veri tabanına erişim sağlamışlar buradan devletin güvenliğine ilişkin bilgileri elde etmişlerdir.
Şüpheliler ayrıca bahsi geçen web sitesinin işleyişini bozmuşlar ve 14-16 Ocak 2012 tarihleri arasında 3 gün süreyle işlemez hale getirmişlerdir.

Şüpheliler elde ettikleri bu bilgileri aşağıda belirtilen 13 adet web sayfasında yayınlamışlardır :

1- www.yellow-hack.net
2- www. undernet.org
3-

Söz konusu bilgilerin yayınlandığı web sitelerine ait ekran çıktıları (screen prints) ekte sunulmuştur.

Suçun hukuki niteliği :

(suçun vasıflandırılması adli makamlarımızın takdirinde olup aşağıdaki suç nitelemeleri fikir vermesi amacıyla yazılmıştır.)

Şüpheliler kamu kurumuna ait bir bilişim sisteminin güvenlik duvarlarını aşarak sisteme insiz erişim sağlamışlar ve sonrasında o sistemi çalışamaz hale getirmişlerdir. Bu eylemler Türk Ceza Kanunu'nda düzenlenen bilişim sistemini engelleme (hacking) suçunu oluşturmaktadır.

Şüpheliler ayrıca buradan elde ettikleri gizli bilgileri 10 adet web sayfasında yayınlayarak ifşa etmişlerdir. Bu eylemler 'Devletin Güvenliğine İlişkin Belgelerin Tahribi-Çalınması' suçunu oluşturmaktadır.

Talep edilen adli yardımlaşma :

Başsavcılığımız tarafından şüpheli hakkında yukarıda belirtilen suçlar nedeniyle soruşturma yapılmaktadır. Soruşturmanın tamamlanabilmesi için --- *(örn, soruşturmaya konu işleme ait IP bilgilerine)* ihtiyaç duyulmaktadır.

Adli yardımlaşma talebinin dayanağı :

Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Adli Yardımlaşma Antlaşması

Garantiler :

Bu talep ceza soruşturması / kovuşturması ile ilgilidir.

Elde edilecek bilgiler yasal sınırlar içinde kullanılacak ilgili kişilerin yasal hakları ihlal edilmeyecektir.

Bu talep; kişiler hakkında politik görüş, din,dil,ırk,cinsiyet,milliyet gibi konularda ayrımcılık yapılmasına ilişkin bir amaç içermez ve bu yönde sonuçlar doğuracak şekilde kullanılmaz.

Sonuç :

Yukarıda belirtilen adli yardım talebinin yerine getirilmesini rica eder ve bu vesileyle yardımlarınız için şimdiden teşekkür eder, en derin saygılarımı sunarım.

(isim, soyadı, sicil no.)
(Cumhuriyet Savcısı)
(İmza)

EKLER:

1) İfade suretleri (Mevcutsa)

2) Davaya konu internet sayfalarının çıktısı (okunaklı ve mümkünse renkli)

3) Bilirkişi raporu (mevcutsa)

4) Yargılamaya esas olan ceza hükümleri (usul hükümlerine gerek yok)

5) Yukarıda sayılı evrakın tercümeleri

Not :

1- Kollukla yapılan yazışmalar, tercümeye gönderme yazıları, sarf kararı gibi yabancı adli makamı ilgilendirmeyen evrak talepnameye eklenmemelidir.

2- Kolay incelenebilmesi için evrak delinerek telli dosyaya takılmalıdır. Evrakı tutturmak için zımba kullanılmamalıdır.

3- Evrak 2 takım halinde düzenlenmeli ve delinerek telli dosyaya takılmalıdır. Evrakta zımba kullanılmamalıdır. Evrakın kolayca tasnifi ve arşivlenmesi için ***her bir takımda*** *evrakın Türkçesi üstte, tercümesi altta olmalıdır.*

Dosya düzeni : Bakanlığa hitaplı üst yazı, 1. takım evrak (Türkçesi üstte / tercümesi altta), 2. takım evrak (Türkçesi üstte / tercümesi altta),

TO THE COMPETENT AUTHOROTIES OF
THE UNITED STATES OF AMERICA

I am investigating a crime committed via ----- (FACEBOOK, GMAİL,.. vb). I am planning to prerapare an MLAT request to be summitted to your authorities but it may take some time. So, I kindly request you to give necessary instruction to preserve the IP and traffic records related the investigation and inform me about the result.

Date of crime :
Suç tarihi

INFOMATIN ABOUT THE VICTIM
Müştekiye ilişkin bilgiler

Name/ surname :
(Adı soyadı)

Victim's e-mail related to the crime : *(suç müştekinin e-maili ile ilgili ise)*
(Müştekinin suça konu e-mail adresi)

Victim's FACEBOOK ID related to the crime :*(suç müştekinin facebook hesabı ile ilgili ise)*
(Müştekinin suça konu facebook ID'si)

Victim's TWITTER ID related to the crime : *(suç müştekinin twitter hesabı ile ilgili ise)*
(Müştekinin suça konu twitter ID'si)

INFORMATION ABOUT THE SUSPECT

Name/ surname :
(Adı soyadı)

Suspect's e-mail related the crime : *(suç şüphelinin gönderdiği e-mail ile ilgili ise)*
(Şüphelinin suça konu e-mail adresi)

Suspect's FACEBOOK ID related to the crime : *(suç şüphelinin facebook hesabı ile ilgili ise)*
(Şüphelinin suça konu facebook ID'si)

Suspect's TWITTER ID related to the crime : *(suç şüphelinin twitter hesabı ile ilgili ise)*
(Şüphelinin suça konu twitter ID'si)

Thank you in advance for your contribution.

İsim / SOYİSİM
Public Prosecutor of ---- (şehir)

Soruşturma aşamasında bilgi-belge temini

Türkiye Cumhuriyeti / /

Cumhuriyet Başsavcılığı

--- Yetkili Adli Makamına

Saygıdeğer meslektaşım,

Sizden aşağıda belirtilen hususlarda adli yardımlaşma talep etmekteyim.

Talebin konusu :

Örn. Bilgi ve belge temini

Soruşturma numarası :

Örn : 2012 / 41975

Suça İlişkin Bilgiler :

Suç Tarihi :

Suçun tanımı : *Dolandırıcılık*

İlgili Ceza Hükümleri : Örn. 5237 Sayılı Türk Ceza Kanunu Madde --

Suçun işleniş şekli :

Örnek olay :

Müşteki M'nin, G. Bankasının Giresun Şubesinde yatırım hesabı bulunmaktadır. Müştekinin yurt dışında olduğu 12.08.2012 tarihinde anılan banka şubesine müşteki tarafından gönderildiği izlenimi verilen bir e-posta gönderilmiştir. E-posta'da 28.08.2012 tarihinde bir teminat yatırmak üzere 100.000 dolar nakit çekme talebi bulunmaktadır. Ertesi gün kendisini H ismiyle tanıtan şüpheli S bankayı arayarak kendisini müştekinin avukatı olarak tanıtmıştır. S elinde M'ye ait vekaletname olduğunu belirterek bu vekaletname gereğince söz

konusu parayı çekeceğini belirtmiştir. S, 16.08.2012 tarihinde banka şubesine gelerek sahte vekaletnameyi ibraz etmiştir. Olaydan şüphelenen banka sorumlusunun polise haber vermesi üzerine S yakalanmıştır. S, e-postayı müştekinin gönderdiğini ve vekaletnamenin müşteki tarafından kendisine verildiğini ileri sürmüştür.

Talep edilen adli yardımlaşma :

Yukarıda anlatılan suç nedeniyle şüpheli X hakkında Cumhuriyet Başsavcılığımızca soruşturma yapılmaktadır. Soruşturmanın tamamlanabilmesi için lütfen aşağıdaki bilgi veya belgeleri Başsavcılığımıza gönderiniz :

1- 12.08.2012 tarihinde sgul@gmail.com hesabından gönderilen e-postanın gönderildiği bilgisayara ait IP kayıtları,
2- IP kayıtları ülkenize ait bir adrese ait ise bu andresteki aboneye ait bilgiler,
3-

Adli yardımlaşma talebinin dayanağı :

Bu kısma isteme dayanak teşkil eden sözleşmenin adı yazılmalıdır.
Taraf olduğumuz çok taraflı ve ikili sözleşmelerin metinlerine ve listesine aşağıdaki linkten ulaşılabilir:
http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adlisbirligi_ceza/cz_istinabe.html

Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi için örnek :
Türkiye ve ....'nın birlikte taraf oldukları Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi (ETS 30)

İkili anlaşma için örnek :
(ABD) : Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Adli Yardımlaşma Antlaşması

Mütekabiliyet uygulamasına örnek:
(Kanada) : Türkiye Cumhuriyeti ile Kanada arasındaki adli yardımlaşma uygulamasına esas olan mütekabiliyet ilkesi

Garantiler :

Bu talep ceza soruşturması / kovuşturması ile ilgilidir.

Elde edilecek bilgiler yasal sınırlar içinde kullanılacak ilgili kişilerin yasal hakları ihlal edilmeyecektir.

Bu talep; kişiler hakkında politik görüş,din,dil,ırk,cinsiyet,milliyet gibi konularda ayrımcılık yapılmasına ilişkin bir amaç içermez ve bu yönde sonuçlar doğuracak şekilde kullanılmaz.

Sonuç :

Yukarıda belirtilen adli yardım talebinin yerine getirilmesini rica eder ve bu vesileyle yardımlarınız için şimdiden teşekkür eder, en derin saygılarımı sunarım.

(isim, soyadı, sicil no.)
(Cumhuriyet Savcısı)
(İmza)

EKLER:

1) Bilirkişi raporu (mevcutsa)
3) İlgili ceza hükümleri
5) Yukarıda sayılı evrakın tercümesi

Soruşturma aşamasında Müşteki
beyanının alınması

Türkiye Cumhuriyeti / /
Cumhuriyet Başsavcılığı

--- Yetkili Adli Makamına

Saygıdeğer meslektaşım,
Sizden aşağıda belirtilen hususlarda adli yardımlaşma talep etmekteyim.

Talebin konusu :
Örn.
Müşteki M'in ifadesinin alınması

Soruşturma numarası :
Örn : 2012 / 41975

Müştekiye ilişkin bilgiler:
Adı-soyadı :
Anne-baba adı :
Doğum yeri / tarihi :
Yurtdışı adresi :

Suça İlişkin Bilgiler :
Suç Tarihi :
Suçun tanımı : *Örn Kasten yaralama*
İlgili Ceza Hükümleri : Örn. 5237 Sayılı Türk Ceza Kanunu Madde 86 /1-3

Suçun işleniş şekli :

Açıklama: Tercümede meydana gelen kayıplar ve anlam kaymaları nedeniyle çok uzun veya devrik cümleler yabancı adli makamlar tarafından anlaşılamamaktadır. Özellikle iddianamelerden kopyalanarak talepnamelere eklenen paragraflarda yer alan sıralı cümle yapısı ve devrik cümleler, tercüme sırasında anlam değişikliğine uğramaktadır. Bu nedenle kısa ve düz cümlelerin kullanıldığı bir anlatım tercih edilmeli, talepnamenin Türkçesinden çok tercümesinin alacağı şeklin önemli olduğu dikkate alınmalıdır.

Örnek olay :

Şüpheli X ile müşteki M arasında daha önceki bir olay nedeniyle husumet bulunmaktadır. Şüpheli X ve müşteki M olay günü karşılaşınca tartışmaya başlamışlardır. Bir süre sonra X yanında getirdiği bıçağı çıkararak M'ye doğru sallamıştır. M bıçağı almak için hamle yapmış ve bıçağın keskin tarafını tutmuştur. Olay yerine gelen kişiler X ve M'yi ayırmışlardır. Olay nedeniyle M'nin elinde 4 cm uzunluğunda bir kesi meydana gelmiştir.

Alınan doktor raporuna göre M basit tıbbı müdahale ile giderilecek şekilde yaralanmıştır.

(Ek--)

Talep edilen adli yardımlaşma :

Başsavcılığımız tarafından şüpheli hakkında yukarıda belirtilen suç nedeniyle soruşturma yapılmaktadır. Müşteki M'nin ülkenizde, yukarıdaki adreste bulunduğu anlaşılmıştır. Soruşturmanın tamamlanabilmesi için müştekinin ifadesinin alınmasına ihtiyaç duyulmaktadır.

Bu nedenle lütfen aşağıdaki işlemleri yerine getiriniz :

Müştekiyi davet ediniz,

Davet üzerine gelmezse (mevzuatınız izin veriyorsa) yetkili adli makamınızın huzuruna zorla getirtiniz,

Kimlik bilgilerini kayda geçiriniz,

Yürütülen soruşturma hakkında kendisine bilgi veriniz,

Ekte tercümesi bulunan Ceza Muhakemesi Kanunu'nun 234. maddesindeki yasal haklarını kendisine anlatınız,

Olayın oluş şekline ilişkin bilgisini ve delillerini sorunuz,

Şüpheliden şikayetçi olup olmadığını sorunuz,

Ayrıca müştekiden aşağıdaki hususları sorunuz : *(olayın aydınlatılması için gerekli olan sorular sırayla yazılmalıdır)*

1-

2-

3-

(Mevcutsa) Müştekiye ekte yer alan bilirkişi raporunu okuyunuz ve rapora itirazı olup olmadığını sorunuz. (Ek --)

*(Mevcutsa)*Müştekiye ekte yer alan daha önceki ifadesini okuyunuz. Şimdiki ifadesi ile önceki ifadesi arasında çelişki varsa çelişkinin nedenini kendisine sorunuz.(Ek --)

Adli yardımlaşma talebinin dayanağı :

Bu kısma isteme dayanak teşkil eden sözleşmenin adı yazılmalıdır.
Taraf olduğumuz çok taraflı ve ikili sözleşmelerin metinlerine ve listesine aşağıdaki linkten ulaşılabilir:
http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adlisbirligi_ceza/cz_istinabe.html

Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi için örnek :
Türkiye ve ……'nın birlikte taraf oldukları Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi (ETS 30)

İkili anlaşma için örnek :
(ABD) : Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Adli Yardımlaşma Antlaşması

Mütekabiliyet uygulamasına örnek:
(Kanada) : Türkiye Cumhuriyeti ile Kanada arasındaki adli yardımlaşma uygulamasına esas olan mütekabiliyet ilkesi

Garantiler :

Bu talep ceza soruşturması / kovuşturması ile ilgilidir.

Elde edilecek bilgiler yasal sınırlar içinde kullanılacak ilgili kişilerin yasal hakları ihlal edilmeyecektir.

Bu talep; kişiler hakkında politik görüş,din,dil,ırk,cinsiyet,milliyet gibi konularda ayrımcılık yapılmasına ilişkin bir amaç içermez ve bu yönde sonuçlar doğuracak şekilde kullanılmaz.

Sonuç :

Yukarıda belirtilen adli yardım talebinin yerine getirilmesini rica eder ve bu vesileyle yardımlarınız için şimdiden teşekkür eder, en derin saygılarımı sunarım.

(isim, soyadı, sicil no.)
(Cumhuriyet Savcısı)
(İmza)

EKLER:

1) İddianame

2) Müştekinin daha önceki ifade sureti (Mevcutsa ve gerekli olduğu ölçüde)

3) Bilirkişi raporu (Mevcutsa ve gerekli olduğu ölçüde)

4) Yargılamaya esas olan yasal hükümler *(CMK'nın 234. Maddesinin metni.)*

5) Yukarıda sayılı evrakın tercümeleri

Şüpheliler için istinabe talepname örneği

(Bilgi- belge temini)

Türkiye Cumhuriyeti / /

Cumhuriyet Başsavcılığı

--- Yetkili Adli Makamına

Saygıdeğer meslektaşım,

Sizden aşağıda belirtilen hususlarda adli yardımlaşma talep etmekteyim.

Talebin konusu :

Örn. : Şüpheli savunmasının alınması

Soruşturma numarası :

Örn : 2012 / 41975

Şüpheliye ilişkin bilgiler:

Adı-soyadı :

Anne-baba adı :

Doğum yeri / tarihi :

Yurtdışı adresi :

Suça İlişkin Bilgiler :

Suç tarihi :

Suçun tanımı : *Örn Kasten yaralama*

İlgili ceza hükümleri : *Örn. 5237 Sayılı Türk Ceza Kanunu Madde 86 /1-3 (usul hükümlerini yazmaya gerek yoktur)*

Suçun işleniş şekli :

Açıklama: Tercümede meydana gelen kayıplar ve anlam kaymaları nedeniyle çok uzun veya devrik cümleler yabancı adli makamlar tarafından anlaşılamamaktadır. Özellikle iddianamelerden kopyalanarak talepnamelere eklenen paragraflarda yer alan sıralı cümle yapısı ve devrik cümleler, tercüme sırasında anlam değişikliğine uğramaktadır. Bu nedenle kısa ve düz cümlelerin kullanıldığı bir anlatım tercih edilmeli, talepnamenin Türkçesinden çok tercümesinin alacağı şeklin önemli olduğu dikkate alınmalıdır.

Örnek olay :

Şüpheli X ile müşteki M arasında daha önceki bir olay nedeniyle husumet bulunmaktadır. Şüpheli X ve müşteki M olay günü karşılaşınca tartışmaya başlamışlardır. Bir süre sonra X yanında getirdiği bıçağı çıkararak M'ye doğru sallamıştır. M bıçağı almak için hamle yapmış ve bıçağın keskin tarafını tutmuştur. Olay yerine gelen kişiler X ve M'yi ayırmışlardır. Olay nedeniyle M'nin elinde 4 cm uzunluğunda bir kesi meydana gelmiştir.

Alınan doktor raporuna göre M basit tıbbı müdahale ile giderilecek şekilde yaralanmıştır.

(Ek --)

Talep edilen adli yardımlaşma :

Başsavcılığımız tarafından şüpheli hakkında kasten yaralama suçu nedeniyle soruşturma yapılmaktadır. Şüpheli X'in ülkenizde, yukarıdaki adreste bulunduğu anlaşılmıştır. Soruşturmanın tamamlanabilmesi için şüphelinin savunmasının alınmasına ihtiyaç duyulmaktadır.

Bu nedenle lütfen aşağıdaki işlemleri yerine getiriniz :

Şüpheliyi davet ediniz,

Davet üzerine gelmezse yetkili adli makamınıza zorla getirtiniz,

Kimlik bilgilerini kayda geçiriniz,

İsnat edilen suçu kendisine anlatınız,

Hiçbir şey söylememe (susma), delil ileri sürme ve bunların toplanmasını isteme, müdafii tayini isteme hakları olduğunu kendisine anlatınız,

Şüpheliden /şüphelilerden yukarıda belirtilen suçlama konusunda savunmasını yapmasını isteyiniz,

Şüpheliden ayrıca aşağıdaki hususları sorunuz : *(olayın aydınlatılması için gerekli olan sorular sırayla yazılmalıdır)*

1-

2-

3-

(Mevcutsa) Şüpheliye ekte yer alan bilirkişi raporunu okuyunuz ve rapora itirazı olup olmadığını sorunuz.

*(Mevcutsa)*Şüpheliye ekte yer alan daha önceki ifadesini okuyunuz. Şimdiki ifadesi ile önceki ifadesi arasında çelişki varsa çelişkinin nedenini kendisine sorunuz.

Adli yardımlaşma talebinin dayanağı :

Bu kısma isteme dayanak teşkil eden sözleşmenin adı yazılmalıdır.
Taraf olduğumuz çok taraflı ve ikili sözleşmelerin metinlerine ve listesine aşağıdaki linkten ulaşılabilir:
http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adlisbirligi_ceza/cz_istinabe.html

Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi için örnek :
Türkiye ve ……'nın birlikte taraf oldukları Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi (ETS 30)

İkili anlaşma için örnek :
(ABD) : Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Adli Yardımlaşma Antlaşması

Mütekabiliyet uygulamasına örnek:
(Kanada) : Türkiye Cumhuriyeti ile Kanada arasındaki adli yardımlaşma uygulamasına esas olan mütekabiliyet ilkesi

Garantiler :

Bu talep ceza soruşturması / kovuşturması ile ilgilidir.

Elde edilecek bilgiler yasal sınırlar içinde kullanılacak ilgili kişilerin yasal hakları ihlal edilmeyecektir.

Bu talep; kişiler hakkında politik görüş,din,dil,ırk,cinsiyet,milliyet gibi konularda ayrımcılık yapılmasına ilişkin bir amaç içermez ve bu yönde sonuçlar doğuracak şekilde kullanılmaz.

Sonuç :

Yukarıda belirtilen adli yardım talebinin yerine getirilmesini rica eder ve bu vesileyle yardımlarınız için şimdiden teşekkür eder, en derin saygılarımı sunarım.

(isim, soyadı, sicil no.)
(Cumhuriyet Savcısı)
(İmza)

EKLER:

1) Şüphelinin daha önceki ifadesi (Mevcutsa ve gerekli olduğu ölçüde)

2) Bilirkişi raporu (mevcutsa ve gerekli olduğu ölçüde)

3) İlgili ceza hükümleri

4) İlgili usul hükmü (Ceza Muhakemesi Kanunu'nun 147. Maddesi)

5) Yukarıda sayılı evrakın tercümeleri

8 BİLİŞİM SUÇLARI SORUŞTURMA MEVZUATI VE UYGULAMASINA İLİŞKİN ÖRNEK MATERYALLER

ÖRNEK OLAY VE SORUŞTURMA AŞAMALARI

ÖRNEK 2

Suç konusu :Hakaret

Olay Yeri : Kadıköy

Olay Tarihi : 25.07.2012 günü

Müşteki :A.O

Müşteki Adresi :Kadıköy

Şüpheli :**abc** ismini kullanan Facebook isimli sosyal paylaşım sitesinden hakaret eden şahıs(açık adresi bilinmiyor)

OLAY ÖZETİ: Müşteki A.O.isimli şahıs avukatı aracılığı ile Kadıköy Cumhuriyet Başsavcılığına 2012/xxxx sayı ile müracaat ederek toplumda saygın bir kişi olduğunu, çok sayıda kitabı ve yayınları bulunduğunu, şüpheli şahsın www.facebook.com isimli internet sitesi üzerinden kendisine" bu geri zekalı adam fetva verirken bunlarda maşallah inşallah diyen ucubeler değilmiydi "diye hakaret ettiğini, şahsın facebook isimli site içerisinden abc@hotmail.com adresini kullandığını davacı ve şikayetçi olduğunu beyan etmiştir.

SNO	SORUŞTURMA AŞAMALARI	YAPILDI
1	Müşteki savcılık makamından havaleli dilekçe ile İlçe Emniyet Müdürlüğüne gelir.	
2	Şikayetçi 5651 sayılı kanun çerçevesinde şikayet aşamalarını tamamlaması istenir.	
3	Müştekinin dilekçedeki/savcılık ifadesindeki bilgiler yeterli değil ise ayrıntılı ifadesi alınır.	
4	Site ile ilgili internet üzerinden www.tib.gov.tr adresinden whois sorgusu yapılır.	
5	Site hakkında Web tespit raporu tanzim edilir. Örnek için **Tıklayınız.**	
6	Şüpheliye ait Microsoft Corporation firmasından alınmış olan e posta adresiyle ilgili kullanıcı log in IP adres bilgi talebinde bulunulur. Örnek için **Tıklayınız.**	
7	E posta yer sağlayıcısı olan firmadan bilgi ve belge talebine cevap alınır.	
8	E posta için gönderilen IP bilgileri ülkemiz saatine çevrilir. Örnek için **Tıklayınız.**	
9	Çözümleme yapılan IP adresi ile ilgili whois sorgusu yapılır. Örnek için **Tıklayınız.**	
10	Şüpheli IP adresi servis sağlayıcıdan sorulur. Örnek için **Tıklayınız.**	
11	Gönderilen kimlik ve adres bilgisi kontrol edilerek şüpheli şahıs tespit edilir.	
12	Şüpheli şahsın konu hakkında ayrıntılı ifadesi alınır.	
13	Olay hakkında tanzim edilen evrak ikmalen/ mevcutlu gönderilir.	

1.4.4.2 Olay 3

Suç konusu : Hakaret ve Tehdit
Olay Yeri : Şişli
Olay Tarihi : 25.09.2012 ve 16.10.2012 tarihleri arası
Müşteki :C.Y.
Müşteki Adresi :Şişli
Şüpheli :**abc@mynet.com** e-posta adresini kullanan şahıs

OLAY ÖZETİ: Müşteki C.Y. isimli şirket avukatı aracılığı ile İstanbul Cumhuriyet Başsavcılığına 2012/xxxx sayı ile müracaat ederek ülkemizin saygın firmalarından biri olduğunu beyan ettiği firmalarına ait info@cy.com.trisimli e-posta adreslerine dilekçelerinde ekli olarak sundukları, tehdit ve hakaret içerikli e-postaların abc@mynet.com isimli e-posta adresini kullanan şahıs tarafından değişik tarihlerde birçok defa gönderildiğini, şahsın her e-posta içeriğinde hakaret ve tehditlerinin dozunu arttırdığını, terbiyesizler, iş yerinizi yakacağım diyerek tehdit ve hakaretlerde bulunduğunu, hakaret ve tehdit içerikli e-postalardan dolayı firma çalışanlarının çok rahatsız olduğunu bahse konu e-posta adresini kullanan şahıstan davacı ve şikayetçi

SNO	SORUŞTURMA AŞAMALARI	YAPILDI
1	Müşteki savcılık makamından havaleli dilekçe ile İlçe Emniyet müdürlüğüne gelir.	
2	Şikayetçi 5651 sayılı kanun çerçevesinde şikayet aşamalarını tamamlaması istenir.	
3	Müştekinin ayrıntılı ifadesi alınır.	
4	Site ile ilgili internet üzerinden www.tib.gov.tr adresinden whois sorgusu yapılır.	
5	Mynet Medya Yayıncılık AŞ isimli firma ülkemizde kayıtlı bir firma olduğu için web tespit raporuna gerek yoktur.	
6	Müşteki tarafından bildirilen şüpheliye ait Mynet Medya Yayıncılık AŞ isimli firmaya ait e posta adresiyle ilgili bilgi ve belge talebinde bulunulur. Örnek için **Tıklayınız.**	
7	E posta yer sağlayıcısı olan firmadan IP bilgisi alınır.	
8	E posta için gönderilen IP bilgileri ülkemiz saatine çevrildi. Mynet isimli firma ülkemizde yayın yapan bir firma olduğu için saat çevrilmesi işlemi yapılmasına gerek yoktur.	
9	Şüphelinin kullanıldığı anlaşılan IP bilgisinin hangi erişim sağlayan firmaya ait olduğu whois sorgusu yapılarak tespit edilir. Örnek için **Tıklayınız.**	
10	IP bilgisi erişim sağlayan firmadan sorularak kullanıcı adres ve kimlik bilgi talebinde bulunulur. Örnek için **Tıklayınız.**	
11	Gönderilen kimlik ve adres bilgisi kontrol edilerek şüpheli şahıs tespit edilir.	
12	Şüpheli şahsın ifadesi alınır.	
13	Olay hakkında tanzim edilen evrak ikmalen/ mevcutlu gönderilir.	

oldukları bildirilmiştir.

1.4.4.3 Olay 3

Suç konusu :Kişisel Bilgilerin Kullanılması, Sahte Profil oluşturulması

Olay Yeri : Bahçelievler

Olay Tarihi :08.11.2012

Müşteki :N.A.

Müşteki Adresi :Bahçelievler

Şüpheli : **www.istanbul.net** sitede müştekinin fotoğrafının kullanılarak aaa isimli üye profilini kullanan şahıs

OLAY ÖZETİ: Müşteki N.A.s isimli şahıs Bakırköy Cumhuriyet Başsavcılığına 2012/xxxx sayı ile müracaat ederek 08.11.2012 akşamı internet ortamında gezindiği esnada kendisine ait olan fotoğrafların **www.istanbul.net** isimli internet sitesinde bulunan aaa isimli profil sayfasında gördüğünü, ayrıca kendisine ait telefon numarasının bu sayfada yayınlandığını, müşteki N.A' nın fotoğrafının kullanılarak aaa isimli profili oluşturan şahıs ya da şahıslardan davacı ve şikayetçi olduğu bildirilmiştir.

SNO	SORUŞTURMA AŞAMALARI	Yapıldı
1	Müşteki savcılık makamından havaleli dilekçe ile İlçe Emniyet müdürlüğüne gelir.	
2	Şikayetçi 5651 sayılı kanun çerçevesinde şikayet aşamalarını tamamlaması istenir.	
3	Müştekinin ayrıntılı ifadesi alınır.	
4	Site ile ilgili internet üzerinden www.tib.gov.tr adresinden whois sorgusu yapılır.	
5	**www.istanbul.net** isimli firma ülkemizde kayıtlı bir firma olduğu için web tespit raporuna gerek yoktur.	
6	Müşteki tarafından bildirilen şüpheliye ait **www.istanbul.net** isimli firmaya ait aaa isimli profille ilgili olarak oluşturulma tarihi, saat, üye isim bilgisi üyelilik ve erişim sağlandığı olay anındaki IP bilgisi varsa, telefon, banka hesap numarası, açık adres ve kimlik bilgisi istenir. Örnek için **Tıklayınız.**	
7	İnternet sitesinden alınan IP bilgisi yine whois sorgusu ile erişim sağlayıcı firma tespit edilir.	
8	**www.istanbul.net** isimli firma ülkemizde yayın yapan bir firma olduğu için saat çevrilmesi işlemi yapılmasına gerek yoktur.	
9	IP bilgisi erişim sağlayan firmadan sorularak kullanıcı adres ve kimlik bilgi talebinde bulunulur. Örnek için **Tıklayınız.**	

10	Gönderilen kimlik ve adres bilgisi kontrol edilerek şüpheli şahıs tespit edilir.	
11	Savcılığın talimatı doğrultusunda başka suç ve suç delillerinin elde edilebilmesi amacıyla şüpheli şahsın ikametine veya işyerine arama el koyma ayrıca arama sonucu elde edilecek olan bilgisayar ve diğer dijital metaryaller üzerinde CMK 134 maddesi uyarınca bilgisayar kütük ve hard disklerinde arama (inceleme) izin talebinde bulunulur. Örnek için **Tıklayınız.**	
12	Arama esnasında tespit edilen dijital metaryallerin imajlarının (birebir kopyalarının) alınarak incelenmesinde kullanılmak üzere ilgili Cumhuriyet Savcılığından el konulan metaryallerin kapasite büyüklüğünün %30 fazlası hard disk talebinde bulunulur. Örnek için **Tıklayınız.**	
13	Tespit edilen dijital metaryaller üst yazı ile içeriğinde inceleme izni bulunan mahkeme kararı ve soruşturma evrakının bir örneği ile Bilişim Suçlarıyla Mücadele Şube Müdürlüğümüze elden teslim edilir. Örnek için **Tıklayınız.**	
14	İnceleme sonucunda hazırlanan rapor ve dijital metaryaller soruşturma birimince geri teslim alınır.	
15	Rapor ve diğer deliller doğrultusunda suçla ilgili şüpheli şahsın ayrıntılı ifadesi alınır.	
16	Olay hakkında tanzim edilen evrak ikmalen/ mevcutlu gönderilir.	

Örnek olay 5:

Suç Konusu : Dolandırıcılık

Olay Yeri : Kadıköy

Olay tarihi : 12.12.2012

Müşteki : yeter SAF

Şüpheli : güveniliradam15 profil ismini kullanan www.sahibinden.com kullanıcısı

Olay özeti: Mağdur Yeter SAF isimli şahıs www.sahibinden.com sitesi üzerinden satılık oto ilanları üzerinde yaptığı araştırmada **güveniliradam15** profil isimli şahsın 12346567893 ilan numarası ile BMW marka 2012 model aracı sattığını gördüğünü, aracı beğenerek ilan kısmında bulunan 0532 222 22 xx telefon numarasından şahsa ulaştığını şahısla anlaşarak, Ziraat Bankasının 005 şubesi 234098766 hesap numarasına 300 TL eft yaptığını, Eft çıktısını ekte sunduğunu, Daha sonra güveniliradam15 profil isimli şüpheliye telefonundan ulaşamadığını, dolandırıldığını anladığını, İlçe Emniyet müdürlüğü Asayiş Büro Amirliğine müracaat ederek şikayetçi olduğu bildirilmiştir.

SNO	SORUŞTURMA AŞAMALARI	Yapıldı
1	Müşteki konu hakkında ayrıntılı ifadesi alınarak savcılık talimatı alınır.	
2	Site ile ilgili internet üzerinden www.tib.gov.tr adresinden whois sorgusu yapılır.	
3	**www.sahibinden.com** isimli firma ülkemizde kayıtlı bir firma olduğu için web tespit raporuna gerek yoktur.	
4	**www.sahibinden.com** isimli firmaya ait şüpheli şahsın kullandığı **güveniliradam15** isimli profille ait üyelilik ve erişim sağladığı IP bilgisi varsa, telefon, banka hesap numarası, açık adres ve kimlik bilgisi istenir. Örnek için **Tıklayınız.**	
5	Şüpheli şahsın kullanmış olduğu telefon numarası ile ilgili GSM firmasından açık adres ve kimlik bilgisi talep edilir.	
6	Ziraat Bankasından şüpheliye ait hesap numarasıyla ilgili kimlik adres ve bahse konu işlem bilgileri talep edilir. Örnek için **Tıklayınız.**	
7	İnternet sitesinden alınan cevabi yazıda IP bilgisi yine whois sorgusu ile erişim sağlayıcı firma tespit edilir. Örnek için **Tıklayınız.**	
8	**www.sahibinden.com** isimli firma ülkemizde yayın yapan bir firma olduğu için saat çevrilmesi işlemi yapılmasına gerek yoktur.	
9	IP bilgisi erişim sağlayan firmadan sorularak kullanıcı adres ve kimlik bilgi talebinde bulunulur. Örnek için **Tıklayınız.**	
10	İlgili firma ve kuruluşlardan gönderilen kimlik ve adres bilgisi kontrol edilerek şüpheli şahıs tespit edilir.	
11	Savcılığın talimatı doğrultusunda başka suç ve suç delillerinin elde edilebilmesi amacıyla şüpheli şahsın ikametine veya işyerine arama el koyma ayrıca arama sonucu elde edilecek olan bilgisayar ve diğer dijital metaryaller üzerinde CMK 134 maddesi uyarınca bilgisayar kütük ve hard disklerinde arama (inceleme) izin talebinde bulunulur. Örnek için **Tıklayınız.**	
12	Arama esnasında tespit edilen dijital metaryallerin imajlarının (birebir kopyalarının) alınarak incelenmesinde kullanılmak üzere ilgili Cumhuriyet Savcılığından el konulan metaryallerin kapasite büyüklüğünün %30 fazlası hard disk talebinde bulunulur. Örnek için **Tıklayınız.**	
13	Tespit edilen dijital metaryaller üst yazı ile içeriğinde inceleme izni bulunan mahkeme kararı ve soruşturma evrakının bir örneği ile Bilişim Suçlarıyla Mücadele Şube Müdürlüğümüze elden teslim edilir. Örnek için **Tıklayınız.**	
14	İnceleme sonucunda hazırlanan rapor ve dijital metaryaller soruşturma birimince geri teslim alınır.	
15	Rapor ve diğer deliller doğrultusunda suçla ilgili şüpheli şahsın ayrıntılı ifadesi alınır.	
16	Olay hakkında tanzim edilen evrak ikmalen/ mevcutlu gönderilir.	

CUMHURİYET BAŞSAVCILIĞINDAN EMNİYETE YAZILAN YAZI

18) Başkasına ait bankamatik kartıyla bankamatikten para çeken kişinin tesbiti.

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO: 2008 /..... **...../..../2008**

T.C.

ESKİŞEHİR

İL EMNİYET MÜDÜRLÜĞÜ

ASAYİŞ ŞUBE MÜDÜRLÜĞÜNE

Müşteki Halkbankası müşterisinin tuzaklama yöntemiyle elde edilen bankamatik kartıyla hesabından para çekilmesi olayı ile ilgili olarak elde edilen kamera görüntülerini içerir CD ile fotoğraflar yazımız ekine gönderilmiştir.

CD ve fotoğraflar üzerinde gerekli incelemelerin yapılarak şüpheli ya da olası şüphelilerin tespit edilerek, bu hususta tanzim edilecek evrakın Cumhuriyet Başsavcılığımıza gönderilmesi, CD üzerinde gerekli incelemeler konusunda teknik olarak imkan bulunmaması halinde, ilgili birimle irtibata geçilerek yazı gereğinin yerine getirilmesi ile düzenlenecek evrakın gönderilmesi rica olunur.

Ünal DOĞAN

Cumhuriyet Savcısı 38087

- EKİ : - Şikayet dilekçesi

6)Başkasına ait msn adresinin hacklenmesi suretiyle 3. kişilerden kontür talebinde bulunan kişinin tesbiti.

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO: 2008 /..... **..../..../2008**

T.C.

ESKİŞEHİR

İL EMNİYET MÜDÜRLÜĞÜ

ASAYİŞ ŞUBE MÜDÜRLÜĞÜ

Müştekiye ait şikayet dilekçesi yazımız ekinde gönderilmiştir.

1- Gerekiyorsa müştekinin şikayet ve delillerinin tespiti,
2- Suç tarihinde ele geçirildiği belirtilen .....@hotmail.com adresini kullanan internet abonesinin kim olduğunun IP vb. bilgilerden yola çıkılarak tespiti,
3- Söz konusu IP vb. bilgilerin kime ait olduğunun internet servisi sağlayan şirketlerden öğrenilmesi,
4- Bu şekilde elde edilmiş kontörlerin hangi telefonlardan kullanıldığının iletişim şirketlerinden öğrenilmesi,
5- Bu şekilde tespit edilecek şüphelilerin Eskişehir ili dahilinde bulunması durumunda müsnet suçla ilgili savunmalarının alınması,
6- Tamamlanacak soruşturma evrakının C.Başsavcılığımızdan alınacak talimat doğrultusunda gönderilmesi rica olunur.

Ünal DOĞAN

Cumhuriyet Savcısı 38087

EKİ : - Müşteki şikayet dilekçesi

- Kontör kartların suretleri

14)Bilişim sistemine hukuka aykırı şekilde giren kişinin kim olduğunun tespit edilmesi

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO: 2008 /..... **...../..../2008**

T.C.

ESKİŞİHİR

İL EMNİYET MÜDÜRLÜĞÜ

ASAYİŞ ŞUBE MÜDÜRLÜĞÜNE

Müştekiye ait şikayet dilekçesi, ekleri ve ifade sureti yazımız ekinde gönderilmiştir.

1- Müştekinin bilişim sistemine hukuka aykırı şekilde girilip girilmediği, işleyişinin engellenip engellenmediği, bilişim sistemindeki verilerin yok edilip edilmediği, bozulup bozulmadığı, sisteminin erişilmez kılınıp kılınmadığı hususlarının tespiti,
2- Müştekinin bilişim sistemine hukuka aykırı şekilde giren kişinin kim olduğunun tespit edilmesi,
3- Gerekiyorsa şüphelinin bilgisayarlarından arama ve inceleme yapılması için tespit edilecek adreslerinde Başsavcılığımız aracılığı ile mahkemesinden bilgisayarlarda arama, inceleme ve el koyma hususunda karar aldırılması, bu karar doğrultusunda gerekli tespitlerin ve incelemelerin yapılması,

Şüphelinin savunmasının alınması, tamamlanacak soruşturma evrakının C.Başsavcılığımızdan alınacak talimat doğrultusunda gönderilmesi rica olunur.

Hasan GÖNEN

Cumhuriyet Savcısı 38780

EKİ ___ :

- Şikayet Dilekçesi ve Ekleri
- İfade Sureti

T.C.
BEYKOZ
CUMHURİYET BAŞSAVCILIĞI
HAZIRLIK BÜROSU

Sayı : 2009/4810 **ELDEN TAKİPLİDİR**

İL EMNİYET MÜDÜRLÜĞÜ
ASAYİŞ ŞUBE MÜDÜRLÜĞÜ
Bilişim Suçları Şube Müdürlüğüne
İSTANBUL

Cumhuriyet Başsavcılığımızca yürütülmekte bulunulan hazırlık soruşturmasına esas olmak üzere;

Şikayetçi ' .... : İnş. Tur. İth. İhr. San. Tic. Ltd. Şti'nin ekli şikayet dilekçesine göre iş yerinde kullanmış oldukları ticari ilişkilerine ait bilgilerin bulunduğu, bilgisayarlarla 12/06/2009 tarihi itibariyle kesin saati verilemeyen bir saatte 10.0.015, 91.191.173.106. IP nolu adreslerden girilerek bilgisayar sistemine zarar verildiğinden bahisle şikayet dilekçesi ekinde bulunan kayıt ve belgelere göre şikayetçi şirketin rızası ve bilgisi dışında TCK 243, 244 maddelerine göre bilişim sistemine girilerek sistemi engelleme, bozma, verileri yok etme, değiştirme ve sistemde haksız şekilde kalma eylemlerini gerçekleştiren kişilerin tespit edilerek, bu şahısların açık kimlik ve adreslerinin tespit edilerek savunmalarının alınması ve düzenlenecek evrakın C.Başsavcılığımıza gönderilmesi rica olunur. 19/06/2009

MURAT BULUT 34264
Cumhuriyet Savcısı

Eki: Şikayet dilekçesi ve ekleri

Katip; İnci Hanım
3220065 dahili 106

TARANDI
KOM-ES : 453061

T.C.
BEYKOZ
CUMHURİYET BAŞSAVCILIĞI
HAZIRLIK BÜROSU

Sayı : 2009/8890 **11/11/2009**

İL EMNİYET MÜDÜRLÜĞÜ
Bilişim Suçları ve Sistemleri Şube Müdürlüğüne
İSTANBUL

Cumhuriyet Başsavcılığımızca yürütülmekte bulunulan hazırlık soruşturmasına esas olmak üzere;

Ekte gönderilen Arama - El Koyma tutanağı ile ilgili olarak, bahsi geçen yerde ekiplerinizce yapılan aramada ele geçirilen deliller üzerinde ne gibi bir işlem yapıldığının araştırılması ve yapılan araştırma ile ilgili düzenlenen belgelerin C.Başsavcılığımıza gönderilmesi rica olunur.

MURAT BULUT 34264
Cumhuriyet Savcısı

BSS Şube Müdürlüğü
Gereği: Bilgi Sistemleri Şb. Md.
Bilgi :
Sayı : 2009/5206
Tarih : 01 Aralık 2009 Paraf :

09/4806
08/2779 Sh. A.ÜNAL

Eki: Arama El koyma tutanağı

EMNİYET MÜDÜRLÜĞÜ
Evrak ve Arşiv Şube Müdürlüğü
25/11/2009 Sayı: 166985
Bilişim Şube Müdürlüğüne
Emn. Md. Md. Yrd. Şb. Md.

8) İnternet üzerinden bir hesaptan diğer hesaba para aktarılması. (2)

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO: 2008 /..... **...../..../2008**

T.C.

ESKİŞEHİR

İL EMNİYET MÜDÜRLÜĞÜ

ASAYİŞ ŞUBE MÜDÜRLÜĞÜNE

Müşteki .....Tic. Ltd. Şti.'nin **Yapı ve Kredi Bankası P.....** şubesindeki .....numaralı hesabına bilgisi dışında internet aracılığı ile **İ..... A.....** adına açılmış **Akbank K.....** şubesindeki ..... nolu hesabına 990,00 YTL, **B..... A....** adına açılmış **Akbank G.....** şubesindeki 186738 nolu hesabına 990,00 ve 50,00 YTL, B..... K..... adına açılmış Türkiye İş Bankası S..... şubesindeki 257476 nolu hesabına 2 defa 900,00YTL ve 1000,00YTL, aktarıldığı ve 1000,00 YTL'nin de Yapı ve Kredi Bankasına ait K..... Ç..... adına düzenlenmiş 5..... 6..... 2..... 2..... nolu kredi kartı ödemesi yapıldığı iddiası ile ilgili şikayet dilekçesi ve ekleri gönderilmiştir.

Soruşturmaya başlanarak;

1- Gerekiyorsa müştekinin şikayet ve delillerinin CMK 234 gereğince tespiti,
2- Müştekinin Yapı ve Kredi Bankası P..... şubesindeki hesabından söz konusu internet havalelerini yapan abonelerin tespiti için havaleyi yapan abonenin IP numarasının ve abonenin tespitine yarayan diğer bilgilerin banka şubesinden alınması,
3- Bu bilgilerin (IP numarası vb.) kime ait olduğunun Bilgi İşlem Şube Müdürlüğü ve Telekom müdürlüğü veya diğer şirketler aracılığı ile tespit edilerek bu şahısların CMK 147 maddesi ve devamı maddeleri gereğince müdafili savunmalarının alınması,
4- Akbank K..... şubesinden İ..... A.....'un hesap numarası adres ve kimlik tespitine ilişkin tüm bilgi ve belgelerin, varsa güvenlik kamerasından görüntülerinde alınarak bu şahsın tespiti ile yakalanıp müsnet suçtan dolayı CMK 147 ve devamı maddeleri gereğince savunmasının alınması,
5- Akbank G..... Şubesinden B..... A....'ın hesap numarası adres ve kimlik tespitine ilişkin tüm bilgi ve belgelerin, varsa güvenlik kamerasından görüntülerinde alınarak bu şahsın tespiti ile yakalanıp müsnet suçtan dolayı CMK 147 ve devamı maddeleri gereğince savunmasının alınması,

6- Türkiye İş Bankası S….. Şubesinden B….. K…..'nın hesap numarası adres ve kimlik tespitine ilişkin tüm bilgi ve belgelerin, varsa güvenlik kamerasından görüntülerinde alınarak bu şahsın tespiti ile yakalanıp müsnet suçtan dolayı CMK 147 ve devamı maddeleri gereğince savunmasının alınması,

7- Yapı ve Kredi Bankası Kredi Kartları Merkezinden 5…. 6…. 2…. 2…. nolu kredi kartı sahibi K…. Ç……'un açık kimlik ve adres tespitine ilişkin tüm bilgi ve belgelerin, varsa güvenlik kamerasından görüntülerinde alınarak bu şahsın tespiti ile yakalanıp müsnet suçtan dolayı CMK 147 ve devamı maddeleri gereğince savunmasının alınması,

8- Müsnet suçla ilgili toplanacak diğer delillerle birlikte soruşturma evrakının C.Başsavcılığımızdan alınacak talimat doğrultusunda gönderilmesi rica olunur.

Hasan GÖNEN
Cumhuriyet Savcısı 38780

EKİ :
- Şikayet dilekçesi ve ekleri

7) İnternet üzerinden bir hesaptan diğer hesaba para aktarılması. (1)

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO: 2008 /..... **...../..../2008**

GARANTİ BANKASI GENEL MERKEZİNE

(KOÇMAN CAD. NO:38 GÜNEŞLİ İSTANBUL)

Müştekiye ait şikayet dilekçesi yazımız ekinde gönderilmiştir.

Müştekiye ait ..... Şubesindeki hesabından ;

1- ..... tarihinde B .... L.... adına 1000 YTL havale edilmesi olayı ile ilgili,
   a. Bu havalenin B .... L.... 'ın neredeki hesabına havale edildiği,
   b. Bu havalenin hangi tarihte yapıldığı
   c. Bu havalenin nasıl yapıldığı, neye istinaden yapıldığı,
   d. Bu paranın alınıp alınmadığı alınmış ise nasıl alındığı,
   e. Havalenin hangi IP numarası üzerinden yapıldığı,
   f. B.... L....'ın açık kimlik ve adres bilgilerinin ne olduğu ,

2- T.... F....'in .... nolu kredi kartı hesabına ..... ve ..... tarihlerinde yapılan transfer ile ilgili olarak,
   a. Bu transferin T..... F....'in hangi şubedeki hesabına yapıldığı,
   b. Bu havalenin nasıl yapıldığı, neye istinaden yapılmış olduğu,
   c. Bu paraların alınıp alınmadığı alınmış ise nereden nasıl alındığı,
   d. Transferlerin hangi IP numarası üzerinden yapıldığı,
   e. T..... F.....'in açık kimlik ve adres bilgilerinin ne olduğu,

hususlarında C.Başsavcılığımıza bilgi verilmesi rica olunur.

Hasan GÖNEN

Cumhuriyet Savcısı 38780

Eki : Şikayet Dilekçesi

T.C.
İSTANBUL VALİLİĞİ
Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.00.58.04.2009/2779 -3u27224813 09/09/2009
Konu : Soruşturma evrakı

BEYKOZ CUMHURİYET BAŞSAVCILIĞINA
(Soruşturma No: 2009/4810)

İlgi : a) Beykoz C. Başsavcılığının 19.06.2009 tarih ve Srş. No: 2009/4810 sayılı yazısı.
b) Teknoas Bilişim Teknolojileri Ltd. Şti. nin 22.07.2009 tarih ve bila sayılı yazısı.

İlgi sayılı yazı ekinde gönderilen ve Müşteki İnş. Tur. San. Tic. adına vekili Av. nail ÖZDERYOL tarafından verilen şikayet dilekçesinde;91.191.173.106 numaralı IP ile şirketin sunucularına uzaktan izinsiz erişim sağlanarak sunuculardaki bazı verilerin değiştirildiği ve silindiği belirtilerek şikayetçi olunmuştur.

Konu hakkında 91.191.173.106 numaralı IP nin kime tahsis edildiği Teknoas Bilişim Teknolojileri Ltd. Şti. isimli şirkete sorulmuştur.Teknoas Bilişim Ltd.Şti. nin ilgi (b) sayılı cevabi yazısında 91.191.173.106 numaralı IP nin **Adres: Teknolojileri Ltd. Şti. Kadıköy/İstanbul** olduğu bildirilmiştir.

Soruşturma evrakında şüpheliye ait olduğu tespit edilen **Kağan Adres: İnternet Teknolojileri Ltd. Şti. Kadıköy/İstanbul** sayılı adrese gidilmiş, yapılan araştırmalarda bahse konu adresin hukuk bürosu olduğu anlaşılmıştır. Teknoas Bilişim Teknolojileri Ltd. Şti. nin ilgi (b) sayılı cevabi yazısında belirtilen telefon numaralarından Kaan isimli şahsa ulaşılamamıştır. Yapılan çalışmalarla ilgili hazırlanan tutanaklar yazımız ekinde sunulmuştur.

Bilgilerinize arz ederim.

Turan ODABAŞ
Bilişim Suçları ve Sistemleri Şb. Md.
3.Sınıf Emniyet Müdürü

EKİ :
1- Soruşturma Evrakı

T.C.
İSTANBUL VALİLİĞİ
Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.00.58.04-2009/5206 — 466261 04/12/2009
Konu : İnceleme Kararı.

270223

BEYKOZ CUMHURİYET BAŞSAVCILIĞINA

İlgi: a) Beykoz C. Başsavcılığının 19.06.2009 tarih ve Srş. No: 2009/4810 sayılı yazısı.
b) Kadıköy 1. Sulh Ceza Mahkemesinin Değ. İş No. 2009/1472 sayılı kararı
c) Beykoz C. Başsavcılığının 11.11.2009 tarih ve Srş. No: 2009/8890 sayılı yazısı.

İlgi (a) sayılı soruşturma kapsamında tespit edilen Şüphelilerin **No: kadıköy/İSATNBUL** işyeri adreslerinde ilgi (b) sayılı karara istinaden arama yapılmış ve WXN509S45476 seri numaralı 500 gb kapasiteli Western Digital marka hard disk bulunarak el konulmuştur.

İlgi (c) sayılı yazıda soruşturma evrakı hakkında bilgi verilmesi istenmektedir. Beykoz C. Başsavcılığının 19.06.2009 tarih ve Srş. No: 2009/4810 sayılı soruşturma evrakı kapsamında elde edilen materyaller ve bilgisayar inceleme raporları C.Başsavcılığınıza gönderilmiştir.

Bilgilerinize arz ederim.

Turan ODABAŞ
Bilişim Suçları ve Sistemleri Şb. Md.
3. Sınıf Emniyet Md.

EKİ : İlgi sayılı yazı fotokopisi.

İst. Emn. Müd. Vatan Cad. B/Blok Giriş Kat Fatih/İSTANBUL Ayrıntılı bilgi için; H.TAŞKIN Polis Memuru Tlf: 0212 636 22 94 Faks : 0212 636 29 83 e-posta: fyurttas@iem.gov.tr.

12)Başkasına ait kredi kartı bilgileri internet üzerinden sipariş verilmek suretiyle alış veriş yapmak

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO: 2008 /.....
...../..../2008

T.C.

ESKİŞEHİR

İL EMNİYET MÜDÜRLÜĞÜ

ASAYİŞ ŞUBE MÜDÜRLÜĞÜNE

N..... K..... isimli şahsın kredi kartı hesabından mail order ile müşteki M..... Bilgisayar' dan H..... Ü..... ve Ö..... U..... ismiyle bilgisayar parçası satın alınması olayı ile ilgili olarak şikayet dilekçesi yazımız ekinde gönderilmiştir.

Soruşturmaya başlanılarak;

1- Gerekiyorsa müştekinin şikayet ve delillerinin tespiti,
2- Müşteki şirkete ait internet sitesinden başkasına ait kredi kartıyla yapılmış olan alışverişlerin tespiti,söz konusu kredi kartı sahibi olan N..... K.....' ın adres ve kimlik bilgilerinin bankadan öğrenilmesi ve konu ile ilgili ifadesinin alınması,
3- İnternet üzerinden verilen sipariş bilgilerine ilişkin IP numarasından yola çıkılarak,IP numarasının kime ait olduğunun internet servisi sağlayan şirketlerden öğrenilmesi bu şekilde şüpheliye ulaşılması,
4- Sipariş sırasında verilmiş bilgilerden yola çıkılarak şüphelilerin tespitine çalışılması,
5- Teslimat adresinden yola çıkılarak şüphelinin tespiti ve teslimatı yapan şahıslardan alınacak bilgi ve eşgal bilgilerinden yola çıkılarak şüphelilerin tespiti,ayrıca teslimata ilişkin kargo teslim tutanaklarının asıllarının elde edilmesi,
6- Şüphelilerin yakalanması durumunda C.Başsavcılığımızdan alınacak talimat doğrultusunda evrakın gönderilmesi rica olunur.

Ünal DOĞAN

Cumhuriyet Savcısı 38087

EKİ : - Şikayet dilekçesi ve ekleri

T.C.
BEYKOZ
CUMHURİYET BAŞSAVCILIĞI
HAZIRLIK BÜROSU

Sayı : 2009/4810

ELDEN TAKİPLİDİR

İL EMNİYET MÜDÜRLÜĞÜ
ASAYİŞ ŞUBE MÜDÜRLÜĞÜ
Bilişim Suçları Şube Müdürlüğüne
İSTANBUL

Cumhuriyet Başsavcılığımızca yürütülmekte bulunulan hazırlık soruşturmasına esas olmak üzere:

Şikayetçi Cem B.... İnş. Tur. İth. İhr. San. Tic. Ltd.Şti'nin ekli şikayet dilekçesine göre iş yerinde kullanmış oldukları ticari ilişkilerine ait bilgilerin bulunduğu, bilgisayarlarla 12/06/2009 tarihi itibariyle kesin saati verilemeyen bir saatte 10.0.015. 91.191.173.106. IP nolu adreslerden girilerek bilgisayar sistemine zarar verildiğinden bahisle şikayet dilekçesi ekinde bulunan kayıt ve belgelere göre şikayetçi şirketin rızası ve bilgisi dışında TCK 243, 244 maddelerine göre bilişim sistemine girilerek sistemi engelleme, bozma, verileri yok etme, değiştirme ve sistemde haksız şekilde kalma eylemlerini gerçekleştiren kişilerin tespit edilerek, bu şahısların açık kimlik ve adreslerinin tespit edilerek savunmalarının alınması ve düzenlenecek evrakın C.Başsavcılığımıza gönderilmesi rica olunur. 19/06/2009

MURAT BULUT 34264
Cumhuriyet Savcısı

Şikayet dilekçesi ve ekleri

2009/2379

1)Başkasına ait kredi kartı bilgileri ile internet üzerinden alış veriş yapılması (1)

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO:2008 /..... **.../.../2008**

T.C.
ESKİŞEHİR
İL EMNİYET MÜDÜRLÜĞÜ
ASAYİŞ BÜRO AMİRLİĞİNE

Müştekiye ait şikayet dilekçesi, ifade sureti ve banka yazıları yazımız ekinde gönderilmiştir.

Müştekinin kredi kartı bilgileri kullanılarak " ..... " isimli işyerinden internet üzerinden müştekinin bilgisi dışında alışveriş yapılmış olmakla;

Söz konusu alışverişlerin kimler tarafından yapıldığının tespiti açısından;

1- Alışveriş yapılan şirket yetkililerinin konuyla ilgili ifade sahibi sıfatıyla alışverişi kimin yaptığı, bu konunun tespitine ilişkin tüm bilgi ve belgelerin elde edilmesi için beyanının alınması,(IP numarası, telefon numarası, kimlik ve adres, ürünün teslim yeri ve adresi)
2- Şirketten elde edilecek bilgilerden yola çıkılarak söz konusu alışverişleri yapan internet abonesinin tespiti için internet servisi sağlayan şirketlerden gerekli bilgi ve belgelerin elde edilmesi
3- Bu şekilde şüpheliye ulaşılması
4- Şüphelinin müdafili savunmasının alınması
5- Tahkikat evrakının Başsavcılığımızdan alınacak talimat doğrultusunda gönderilmesi rica olunur.

Ünal DOĞAN
Cumhuriyet Savcısı 38087

EKİ :

- Şikayet dilekçesi, ifade sureti ve banka yazıları

15)Cep bank yöntemiyle para havale eden kişinin kim olduğunun tespit edilmesi

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO: 2008 /..... **...../..../2008**

T.C.

ESKİŞİHİR

İL EMNİYET MÜDÜRLÜĞÜ

ASAYİŞ ŞUBE MÜDÜRLÜĞÜNE

Müşteki **C..... İ....' nin, Garanti Bankası K....** Şubesindeki hesabından bilgisi dışında internet aracılığı ile **cep bank yöntemiyle 150 YTL** tutarın **0 543 ... .** nolu cep telefonuna transfer edilerek çekilmesi iddiasıyla ilgili müştekinin şikayet dilekçesi, ifadesi ve transferin yapıldığı tarih ve IP numaralarını gösterir banka yazısı yazımız ekinde gönderilmiştir.

Soruşturmaya başlanılarak;

1- Gerektiğinde soruşturma konusu ile ilgili bilgi ve belgelerin bankadan elde edilmesi,
2- Transferi yapan internet abonesinin IP numarası vb. bilgilerden yola çıkılarak kim olduğunun tespiti,
3- Söz konusu IP numarasının kimlere ait olduğunun internet servisi sağlayan şirketlerden öğrenilmesi,
4- Transferin yapılmış olduğu cep telefonunun kime ait olduğu hususunun açık adres ve kimlik bilgilerinin iletişim şirketinden öğrenilmesi,
5- Söz konusu paranın hangi ATM den çekildiği ve suç tarihinde (paranın çekim tarihinde) varsa mevcut ATM görüntülerinin de elde edilerek şüpheliye ulaşılması
6- Şüpheli veya şüphelilere ulaşılması durumunda savunmalarının alınarak C.Başsavcılığımızdan alınacak talimat doğrultusunda evrakın gönderilmesi rica olunur.

Ünal DOĞAN

Cumhuriyet Savcısı 38087

- EKİ : - Şikayet dilekçesi
  -İfade Sureti
  -Banka Yazısı

5)İçerisinde suç unsuru bulunan e-maillerin göndericisinin tesbiti.

T.C.

ESKİŞEHİR

CUMHURİYET BAŞSAVCILIĞI

SORUŞTURMA NO:2008 /..... **...../..../2008**

T.C.
ESKİŞEHİR
İL EMNİYET MÜDÜRLÜĞÜ
ASAYİŞ ŞUBE MÜDÜRLÜĞÜNE

Yapılmakta olan bir soruşturmayla ilgili olarak;

Yazımız ekinde gönderilen elektronik mesajların hangi abone tarafından gönderildiğinin tespiti,

Bu hususun tespiti açısından ;

İlgili internet servisi sağlayan şirketlerden ve telefon şirketlerinden IP vb. numaraların ve bu numaraların kimlere ait olduğu hususundaki bilgilerin elde edilmesi,

Tespit edilecek şüphelinin savunmasının alınması, tamamlanacak soruşturma evrakının Başsavcılığımızdan alınacak talimat doğrultusunda gönderilmesi rica olunur.

Hasan GÖNEN
Cumhuriyet Savcısı 38780

EKİ : - Müşteki şikayet dilekçesi
- Elektronik mesaj

WHOİS SORGUSU

OnlineNIC Whois Search Results

Registrant :

Bilisim San. Tic. Ltd. Sti. info@ .com +9.02122886060
Bilisim San. Tic. Ltd. Sti.
Sk Mecidiyekoy
Istanbul N/A TR 34394

Domain Name: .COM { .com }
Registration Date : 2004-1-13
Expiration Date : 2018-1-13
Last update :2011-12-21 10:15:12

Domain Name Server:
ns3. .com
ns4. com

Administrator:
info@ .com +9.02122886060
Bilisim San. Tic. Ltd. Sti.
Sk No Kat Mecidiyekoy
istanbul NA TR 34394

Technical Contact:
info@ .com +9.02122886060
Bilisim San. Tic. Ltd. Sti.
Sk No Kat Mecidiyekoy
istanbul NA TR 34394

Billing Contact:
Arif info@ .com +9.02122886060
Bilisim San. Tic. Ltd. Sti.
Sk No Kat Mecidiyekoy
istanbul NA TR 34394

SİTE BİLGİLERİ SORGU SAYFASI
7 Kasım, 2012 14:44:14

http://ww .com/
Sorgula
Ayrıntılı Sorgula

SİTE BİLGİLERİ
Yazdır

Url	http://www .com/
Alan Adı	www .com
Şehir/Ülke	Istanbul / Türkiye
Sitenin IP'leri	89.106.30.106
Yer Sağlayıcı	Bilisim Limited Sirketi
Alan Adı Durumu	Site Kayıtlı
Alan Adı Sunucuları	ns3. .com
Alan Adı Kayıt Başlangıç Tarihi	1/13/2004
Alan Adı Kayıt Bitiş Tarihi	01/13/2018
Alan Adı Kayıt Firması	
Alan Adı Kayıt Ettiren	Bilisim San. Tic. Ltd. Sti. info@projehaber.com +9.02122886060 +9.02123473784

ALAN ADI KİMLİK BİLGİLERİ

The Data in OnlineNIC's WHOIS database is provided by OnlineNIC for information purposes, and to assist persons in obtaining information about or related to a domain name registration record. OnlineNIC does not guarantee its accuracy. By starting a WHOIS query, you agree that you will use this Data only for lawful purposes and that, under no circumstances will you use this Data to:
(1)allow, enable, or otherwise support the transmission of mass unsolicited,commercial advertising or solicitations via e-mail(spam).
(2)enable high volume,automated, electronic processes that apply to OnlineNIC Inc.(or its systems).

OnlineNIC reserves the right to modify these terms at any time.
By starting this query, you agree to abide by this policy.

Registrant:
Bilisim San. Tic. Ltd. Sti. info@ .com +9.02122886060 +9.02123473784
Bilisim San. Tic. Ltd. Sti.
Polat Mecidiyekoy Is Merkezi No:
istanbul,N/A,TR 34394

Domain Name com
Record last updated at 2012-09-07 12:20:52
Record created on 1/13/2004
Record expired on 01/13/2018

Domain servers in listed order:
ns3.projehaber.com ns4.projehaber.com

Administrator:
(Sk. Polat Mecidiyekoy Is Merkezi No:
istanbul
N/A,
TR
34394

name:(Bilisim San. Tic. Ltd. Sti.)
mail:(info@ .com) +9.02122886060
+9.02123473784
Bilisim San. Tic. Ltd. Sti.

Technical Contactor:
(Sk. Polat Mecidiyekoy Is Merkezi No:
istanbul
N/A,
TR
34394

name:(Bilisim San. Tic. Ltd. Sti.)
mail:(info@ com) +9.02122886060
Bilisim San. Tic. Ltd. Sti.

Billing Contactor:
Sk. Polat Mecidiyekoy Is Merkezi No:
istanbul
N/A,
TR
34394

name:(Bilisim San. Tic. Ltd. Sti.)
mail:(info@ .com) +9.02122886060
+9.02123473784
Bilisim San. Tic. Ltd. Sti.

Registration Service Provider:
name: Bilisim Ltd. Sti.
tel: +9.0212288606
fax: +9.02123473784
web:http://www.anba.com.tr


IP TESPİT
İSTEĞİ

EK 7

T.C.
İSTANBUL VALİLİĞİ
İl Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.58858-(62217)-**2012/....** .../10/2012

Konu : Bilgi Talebi

WWW.İSTANBUL.NET'E

Eski Üsküdar Cad. VIP Center No:10 Kat: 7 Ataşehir/İST

İlgi : Bakırköy C. Başsavcılığının .../.../2012 tarihli ve 2012/xxxx sayılı yazısı.

İlgi sayılı tahkikata esas olmak üzere; **www.istanbul.net** isimli internet sitenizde bulunan "**awaşim"** kullanıcı adlı üyenizin;

- Üyeliğini ilk oluştururken sisteminizde belirtilen şahıs bilgileri,
- Sisteminize erişim sağlarken kullanmış olduğu IP numaralarının tarih ve saat bilgileri ile birlikte,

tespit edilerek düzenlenecek olan evrakın **İstanbul Emniyet Müdürlüğü Bilişim Suçlarıyla Mücadele Şube Müdürlüğüne** gönderilmesi hususunda;

Bilgi ve gereğini arz/rica ederim.

.....
İlçe Emniyet Müdürü
3. Sınıf Emniyet Müdürü

EK :
İlgi sayılı yazı (1 Sayfa)

DAĞITIM :
Gereği :
www.istanbul.net'e

Bilgi :
Bakırköy Cumhuriyet Başsavcılığına

İst. Emn. Müd., BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat: T. ÇETİN P.M.
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@iem.gov.tr

İK 6

T.C.
KADIKÖY KAYMAKAMLIĞI
İlçe Emniyet Müdürlüğü

K - Q
TSE-ISO-EN
9000

Sayı : B.05.1.EGM.4.34.58858-(62217) - **2012/....** .../.../2012

Konu : Bilgi Talebi

MYNET MEDYA YAYINCILIK ULUSLARARASI ELEKTRONİK BİLGİLENDİRME VE HABERLEŞME HİZMETLERİ AŞ'YE

Koru Cad. Arı Teknokent B Blok Kat:6 İ.T.Ü. kampus içi Maslak

İlgi : İstanbul Cumhuriyet Başsavcılığının .../.../2012 tarihli ve 2012/xxxx sayılı yazısı.

İlgi sayılı yazı ile Şube Müdürlüğümüzce yürütülmekte olan soruşturmaya esas olmak üzere; kurumunuz tarafından verilmiş olan **abc@mynet.com**isimli e-posta adresi için;

- İlk açılış IP numarasının tarih/saat bilgileri ile birlikte tespit edilerek.
- E-posta hesabına erişim sağlanırken sisteminize bırakmış IP numaralarının tarih/saat bilgileri ile birlikte tespit edilerek.
- Msn Messenger servisinize erişim sağlanırken sisteminize bırakmış olduğu IP numaralarının tarih/saat bilgileri ile birlikte tespit edilerek.
- E-posta adreslerine ait "contactlist" lerin çıkartılarak,

Hazırlanacak olan raporun **İlçe Emniyet Müdürlüğümüze** gönderilmesi hususunda gereğini Mynet Medya Yay.'dan, bilgi edinilmesini İstanbul Cumhuriyet Başsavcılığından:

Arz/rica ederim.

...
İlçe Emniyet Müdürü
3. Sınıf Emniyet Müdürü

EK :
İlgi sayılı yazı (1 Sayfa)

DAĞITIM :
Gereği :
Mynet Medya Yay.' a

Bilgi :
İstanbul Cumhuriyet Başsavcılığına

İst. Emn. Müd., BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat: İ. ÇETİN P.M.
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@ism.gov.tr

EK 2

T.C.
KADIKÖY KAYMAKAMLIĞI
İlçe Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.58858-(62217) - **2012/....** .../.../2012

Konu : Bilgi Talebi

MİCROSOFT CORPORATIONA

BellevueResidance Levent Mah. Aydın Sok. No:7 34340
Levent / Beşiktaş

İlgi : Kadıköy Cumhuriyet Başsavcılığının .../.../2012 tarihli ve 2012/xxxx sayılı yazısı.

İlgi sayılı yazı ile Şube Müdürlüğümüzce yürütülmekte olan soruşturmaya esas olmak üzere; kurumunuz tarafından verilmiş olan **abc@hotmail.com**isimli e-posta adresi için;

- İlk açılış IP numarasının tarih/saat bilgileri ile birlikte tespit edilerek,
- E-posta hesabına erişim sağlanırken sisteminize bırakmış IP numaralarının tarih/saat bilgileri ile birlikte tespit edilerek,
- Msn Messenger servisinize erişim sağlanırken sisteminize bırakmış olduğu IP numaralarının tarih/saat bilgileri ile birlikte tespit edilerek,
- E-posta adreslerine ait "contactlist" lerin çıkartılarak,

Hazırlanacak olan raporun **İlçe Emniyet Müdürlüğümüze** gönderilmesi hususunda gereğini Microsoft Corporation'dan, bilgi edinilmesini Kadıköy Cumhuriyet Başsavcılığından;
Arz/rica ederim.

.....
İlçe Emniyet Müdürü
3. Sınıf Emniyet Müdürü

EK :
İlgi sayılı yazı (1 Sayfa)

DAĞITIM :
Gereği :
Microsoft Corporationa

Bilgi :
Kadıköy Cumhuriyet Başsavcılığına

İst. Emn. Müd., BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat: T. ÇETİN P.M.
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@iem.gov.tr

WEB SİTESİ İNCELEME RAPORU

Ek 1

WEB SİTESİ İNCELEME RAPORU

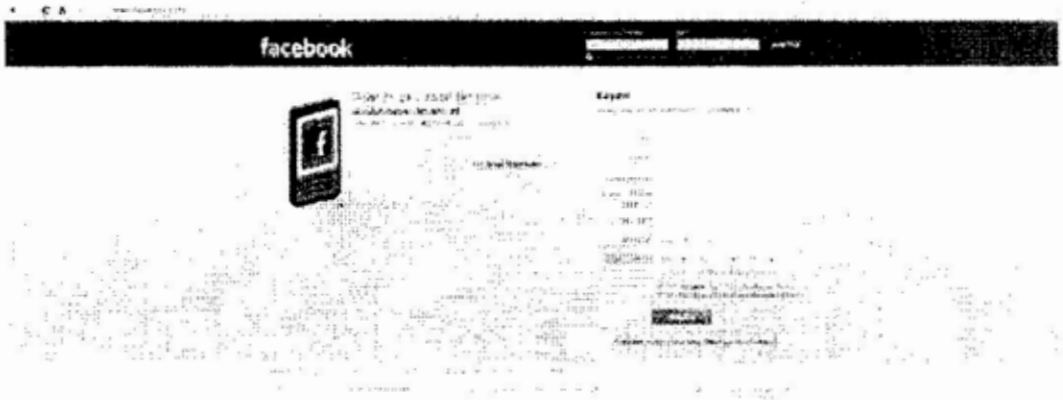
İNCELEMEYİ TALEP EDEN : Kadıköy Cumhuriyet Başsavcılığı

EVRAKTARİHİ : .../.../2012 Soruşturma No: 2012/xxxx

KİMLİK VE ADRES TESPİTİ İSTENİLEN WEB SİTESİNİN

SİTEADRESİ : **https://www.facebook.com/**
YAYIN YAPTIĞI IP NUMARASI : **66.220.149.88**
HOSTİNG FİRMASI : Palo Alto / Amerika Birleşik Devletleri, Facebook, Inc.
ALAN ADI TESCİL BİLGİLERİ : **Created on.....: 1997-03-28.**
Expires on.....: 2020-03-29.
Recordlastupdated on..: 2012-09-28.

EKRAN GÖRÜNTÜSÜ :



SONUÇ:
Site içeriği incelendiğinde **https://www.facebook.com/** isimli sitenin sosyal paylaşım sitesi olduğu görülmüş, domain ve whois kayıtları hakkında yapılan araştırmada yurt dışında bulunan firma sunucuların barınma hizmeti aldığı anlaşılmış olup gerekli bilgi ve belgelerin temin edilebilmesi ancak adli istin yoluyla mümkün olmaktadır.

Arz ederim

TESPİTİN YAPILDIĞI TARİH SAAT : 22/11/2012 saat:16:10

Taner ÇETİN
Polis Memuru

SİTELERİ ZİYARET EDİLEN IP ADRESLERİ

Ek 12

T.C.
İSTANBUL VALİLİĞİ
İl Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.58858-(62217)-**2012/xxxx** .../09/2012

Konu : Bilgi ve Belge Talebi

WWW.SAHİBİNDEN.COM'A

(Değirmen Sok. Nida Kule Kat:5 Kozyatağı - İSTANBUL)

İlgi : Bakırköy Cumhuriyet Başsavcılığının 10/08/2012 tarihli ve 2012/xxxx sayılı yazısı.

İlgi sayılı yazı ile Şube Müdürlüğümüzce yürütülmekte olan bir tahkikata esas olmak üzere; **www.sahibinden.com** isimli internet sitesine **k@hotmail.com** mail adresi ile giriş yapan üyenizin **08/08/2012** tarihinden günümüze kadar erişim sağlayan şahıslara ait IP numaralarının **tarih ve saat** bilgileri ile tespit edilerek, düzenlenecek olan evrakın **İstanbul Emniyet Müdürlüğü Bilişim Suçlarıyla Mücadele Şube Müdürlüğüne** gönderilmesi hususunda:

Bilgi ve gereğini arz/rica ederim.

.....
Bilişim Suçlarıyla Mücadele Şube Müdürü
3. Sınıf Emniyet Müdürü

EK:
İlgi sayılı yazı (1 Sayfa)

DAĞITIM:
Gereği:
www.sahibinden.com'a

Bilgi:
Bakırköy Cumhuriyet Başsavcılığına

İst. Emn. Müd.. BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat: İ. ÇETİN P.M.
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@iem.gov.tr

T.C.
İSTANBUL VALİLİĞİ
Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.00.58.04.2009/2779 .../07/2009
Konu : Bilgi Talebi

TEKNOAS BİLİŞİM TEKNOLOJİLER
(İbrahim Gökçen Bulvarı Onur Sk. No:5/A Manisa)

İlgi : Beykoz c. Başsavcılığının 2009/4810 sayılı soruşturması

İlgi sayılı yazıya istinaden yapılan bir soruşturma kapsamında şirketinize ait 91.191.173.106 IP numarasını 01.06.2009 günü saat 15:36.43 ile 12.06.2009 tarihleri arasında kullanan kullanıcılarınız tespit ile, .ih.İhr. San.ve Tic. Ltd. Şti. isimli firmanın şirketinizden ne tür bir hizmet aldığı ve hizmet aldı ise bu şirket ile şirketiniz arasındaki tüm resmi belgeler ile hosting vb. hizmetler kapsamında 01.06.2009 tarihi ve 13.06.2009 tarihleri arasında serverlarınıza erişim yaparken kullandıkları IP numaralarının tarih ve saatleri ile birlikte tespit edildikten sonra **ÇOK ACELE İstanbul İl Emniyet Müdürlüğü Bilişim Suçları ve Sistemleri Şube Müdürlüğü'ne** önce faks ardından da posta yolu ile gönderilmesi hususunda:

Gereğini rica ederim.

Hüseyin MERAŞ
İl Emniyet Müdürü a.
İl Emniyet Müdür Yardımcısı
2. Sınıf Emniyet Müdürü

EK:
1-İlgi sayılı yazı fotokopisi (1 Sayfa)

İstanbul Emniyet Müdürlüğü Bilişim Suçları ve Sistemleri Şb.Md. Bilişim Suçları Br. Amr. B. Blok Vatan Caddesi FATİH/İSTANBUL
İrtibat Pol.Me.: M.SANSAR E.-Posta: bilisimsuclari@iem.gov.tr Tlf: 0 212 636 22 94 Faks: 0 212 636 29 83

T.C.
İSTANBUL VALİLİĞİ
İl Emniyet Müdürlüğü

K-Q TSE-ISO-EN 9000

Sayı : B.05.1.EGM.4.34.00.11.02.2007/(07-Ds. CBS:476)31050-2083 17/08/2007

Konu : Bilgi Talebi

BEYOĞLU CUMHURİYET BAŞSAVCILIĞINA
(SORUŞTURMA NO : 2007/17464

İlgi : 02.08.2007 tarih ve 2007/17464 soruşturma sayılı yazınız,

İlgi sayılı yazı ile, Müşteki [redacted] Reklamcılık ve Tic.A.Ş'ye ait **www.** [redacted] **:om** isimli internet sitesine internet üzerinden DDOS atak denilen sanal saldırı yapmak suretiyle bilişim sisteminin işleyişini engelleyen, sistemi işlemez hale getiren ve sisteme kayıtlı üyelerin sisteme girişlerini engelleyen bilgisayar kullanıcılarının açık kimlik ve adres bilgilerinin tespit edilerek Cumhuriyet Başsavcılığınıza gönderilmesi istenmiştir.

Soruşturma kapsamında değerlendirilmek üzere; [redacted]**@hotmail.com** isimli Hotmail adresinin oluşturulması esnasında verilen kullanıcı bilgileri ile e-mail adresinin **10.07.2007 – 17.08.2007** tarihleri arasındaki kullanımı esnasında düşen IP numaralarının tespit edilerek gelen görevlimize elden teslim edilmesi için yazımızın **Microsoft Corporation ' na** havalesini arz ederim.

Mustafa KÖSE
Asayiş Şube Müdürü
3 Sınıf Emniyet Müdürü

MİCROSOFT CORPORATION

İstenilen bilgi ve belgelerin tespit edilerek gelen görevliye elden verilmesi veya 0212 214 47 00 numaralı faksa gönderilmesi rica olunur.

17/08/2007
Cumhuriyet Savcısı

17/07/2007 Büro Memuru :M.CENGİZ
.../07/2007 İnt.Bil.Suç.Kıs.A.:D.AY

17.08.07
Microsoft
BİLGİSAYAR YAZILIM HİZMETLERİ LTD.ŞTİ.
Barbaros Plaza İş Merkezi Emirhan Cad.
No:145/C 34349 Dikilitaş - İSTANBUL
Boğaziçi Kurumlar V.D. 621 00[redacted]498

Asayiş Şube Müdürlüğü Arge Br. Amirliği İnternet ve Bilişim Suçları Kısmı Gayrettepe/İstanbul
Ayrıntılı Bilgi İçin:P.M.MUHAMMET CENGİZ
Telefon : **0212 214 43 96** Fax : **0212 214 47 00**

26)Bir bilişim sisteminin işleyişini engelleyen kişinin tesbiti

T.C.
ESKİŞEHİR VALİLİĞİ
Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.26.00.16.12. .../../2008
15111-Bil.Suç.Br.A.2796/07
Konu : Bilgi Talebi.

CUMHURİYET BAŞSAVCILIĞINA
ESKİŞEHİR

İlgi : 20.08.2007 tarih ve Soruşturma No:2007/.... sayılı talimat yazınız.

İlgi sayılı yazınız ekinde Eskişehir Vergi Dairesi Başkanı Fethi AYGÜN'ün dilekçesi KOM Şube Müdürlüğümüz Bilişim Suçlarına gönderilmiş olmakla, gerekli tahkikatın yapılması istenmiştir.Şikayetçinin dilekçesi incelendiğinde; **Organize Sanayi Bölgesinde bulunan eso_es.net'e ait server'dan, http://www.evdb.gov.tr/ adresi ile 212.174.217.107 nolu IP'den yayın yapmakta olan Eskişehir Vergi Dairesi Başkanlığına ait sitenin, 25.07.2007 tarihinde Saat: 08:15 sıralarında yetkisiz kişi veya kişilerce çökertildiğinin tespit edildiği** belirtilmiştir.

Konuyla ilgili yapılacak tahkikata esas teşkil etmek üzere;

1.) **http://www.evdb.gov.tr/** adresine yetkisiz erişim sağlayan bilgisayar/bilgisayarların IP numaralarının (Tarih, saat, dakika ve saniye bilgileri ile birlikte) çıkartılması,

2.) Söz konusu sitenin ne şekilde çökertildiği (Teknik saldırı sonucu mu veya başka bir sebeple mi), sitenin devre dışı kalıp kalmadığı,

3.) Sitenin halen faal olup olmadığı ile olayın çözümüne yarayacak her türlü bilgi ve belgenin Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğine gönderilmesi için Eskişehir Bilişim İletişim Sanayi ve Ticaret A.Ş.'ye talimat verilmesini arz ederim.

Kemal KIZILBABA
KOM Şube Müdür V.
Başkomiser

ESKİŞEHİR BİLİŞİM İLETİŞİM SANAYİ VE TİCARET A.Ş.'YE
(Organize Sanayi Bölgesi 15. Cadde)
26110 / ESKİŞEHİR

Yukarıda istenen hususların ivedilikle çıkartılarak Eskişehir Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğüne gönderilmesi rica olunur. ../../2008

Ünal DOĞAN
Cumhuriyet Savcısı-38087

BİLGİSAYAR KÜTÜKLERİNDE ARAMA KARARI TALEBİ

Kadıköy Sor. No: 2009/57645

T.C.
BEYKOZ
CUMHURİYET BAŞSAVCILIĞI
HAZIRLIK BÜROSU

Sayı : 2009/4810 **15/10/2009**
Konu : Hukuk bürosunda ve bilgisayar kütüklerinde arama kararı talebi

CUMHURİYET BAŞSAVCILIĞI'NA
KADIKÖY

Cumhuriyet Başsavcılığımızca yürütülmekte bulunulan hazırlık soruşturmasına esas olmak üzere;

Hastanesi İnş. Tur. Ith. Ihr. San. Tic. Ltd. Şirketinin ekti şikayet dilekçesine göre iş yerinde kullanmış oldukları ve ticari ilişkilerine ait bilgilerin de bulunduğu bilgisayarlara 12/06/2009 tarihinde kesin saati belirlenemeyen bir saatte 91.191.173.106 IP numarası üzerinden Caferağa mahallesi Sakızgülü sokak no 17/7 Kadıköy adresindeki bilgisayar üzerinden 91.191.173.106 IP numarası kullanılarak izinsiz erişim sağlanarak bilgisayar harddiskinde bulunan bir kısım verilerin ve ticari bilgilerin yok edildiğinden bahisle şikayetçi olunduğu

Ekteki şikayet dilekçesi içeriğine göre 12/06/2009 tarihinde saati belirlenemeyen bir zamanda 91.191.173.106 IP numarası kullanıcısının ekteki İstanbul Emniyet Müdürlüğünün 09/09/2009 tarihli yazısına göre **mahallesi sokak no Kadıköy İstanbul** adresinde bulunduğu ve bu adresin polis tutanağına göre halen **hukuk bürosu** olarak kullanıldığından bahisle adli kolluk yönetmeliğinin madde 13 ile CMK 134. maddelerine göre söz konusu adresteki bilgisayarlar, bilgisayar proğramları ve kütüklerinde arama ve el koyma kararının Sulh Ceza Mahkemesinden alınarak belirtilen adreste gündüzleyin bir kereye mahsus arama yapılmasına karar verilmesi, talimatın ikmalen yerine getirilmesi ve düzenlenecek evrakların C.Başsavcılığımıza gönderilmesi rica olunur.

MURAT BULUT 34264
Cumhuriyet Savcısı

EKİ: 4 adet

T.C.
BEYKOZ
CUMHURİYET BAŞSAVCILIĞI
HAZIRLIK BÜROSU

Sayı : 2009/4810 **15/10/2009**
Konu : Hukuk bürosunda ve bilgisayar kütüklerinde arama kararı talebi

CUMHURİYET BAŞSAVCILIĞI'NA
KADIKÖY

Cumhuriyet Başsavcılığımızca yürütülmekte bulunulan hazırlık soruşturmasına esas olmak üzere;

İnş. Tur. Ith. Ihr. San. Tic. Ltd. Şirketinin ekti şikayet dilekçesine göre iş yerinde kullanmış oldukları ve ticari ilişkilerine ait bilgilerin de bulunduğu bilgisayarlara 12/06/2009 tarihinde kesin saati belirlenemeyen bir saatte 91.191.173.106 IP numarası üzerinden mahallesi sokak no Kadıköy adresindeki bilgisayar üzerinden 91.191.173.106 IP numarası kullanılarak izinsiz erişim sağlanarak bilgisayar harddiskinde bulunan bir kısım verilerin ve ticari bilgilerin yok edildiğinden bahisle şikayetçi olunduğu

Ekteki şikayet dilekçesi içeriğine göre 12/06/2009 tarihinde saati belirlenemeyen bir zamanda 91.191.173.106 IP numarası kullanıcısının ekteki İstanbul Emniyet Müdürlüğünün 09/09/2009 tarihli yazısına göre **mahallesi sokak no Kadıköy İstanbul** adresinde bulunduğu ve bu adresin polis tutanağına göre halen **hukuk bürosu** olarak kullanıldığından bahisle adli kolluk yönetmeliğinin madde 13 ile CMK 134. maddelerine göre söz konusu adresteki bilgisayarlar, bilgisayar proğramları ve kütüklerinde arama ve el koyma kararının Sulh Ceza Mahkemesinden alınarak belirtilen adreste gündüzleyin bir kereye mahsus arama yapılmasına karar verilmesi, talimatın ikmalen yerine getirilmesi ve düzenlenecek evrakların C.Başsavcılığımıza gönderilmesi rica olunur.

MURAT BULUT 34264
Cumhuriyet Savcısı

Evrakı elden teslim aldım.
Av. Teknarl
15.10.2009

EKİ: 4 adet

IP NUMARASINDAN ŞAHIS TESPİT TALEBİ

EK 15

T.C.
KADIKÖY KAYMAKAMLIĞI
İlçe Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.58858-(62217)-**2012/....** .../10/2012

Konu : Bilgi ve Belge Talebi

TURKCELL İLETİŞİM HİZMETLERİ AŞ'YE

Maltepe Mah. Davut paşa Cd. Serçekale Sok. No:2 Zeytinburnu

İlgi : Bakırköy C. Başsavcılığının .../.../2012 tarih ve 2012/xxxx sayılı yazısı.

İlgi sayılı yazı ile Bilişim Suçlarıyla Mücadele Şube Müdürlüğümüzce yürütülmekte olan ilgili soruşturmaya esas olmak üzere; aşağıda belirtilen IP numaralarını kullanan **özel ve tüzel kişilerin telefon, adres ve kimlik** bilgilerine ihtiyaç duyulmaktadır.

IP NUMARASI	TARİH	SAAT
212.253.112.25	.../.../...	...:...

Mevcut bilgilerin tespit edilerek **İlçe Emniyet Müdürlüğüne** gönderilmesi hususunda:
Bilgi ve gereğini arz/rica ederim.

.....
İlçe Emniyet Müdürü
3. Sınıf Emniyet Müdürü

EK:
İlgi sayılı yazı (1 Sayfa)

DAĞITIM :
Gereği:
TurkcellİletişimHizmetleri AŞ'ye

Bilgi:
Bakırköy Cumhuriyet Başsavcılığına

İst. Emn. Müd., BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat. T. ÇETİN P.M.
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@iem.gov.tr

FK 5

T.C.
KADIKÖY KAYMAKALIĞI
İlçe Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.58858-(62217)-**2012/.....** .../01/2013

Konu .: Bilgi ve Belge Talebi

TÜRK TELEKOMÜNİKASYON AŞ'YE
(İstanbul 1.Bölge Müdürlüğü)

İlgi : .....Cumhuriyet Başsavcılığının 05/09/2012 tarihli ve 2012/..... sayılı yazısı.

İlgi sayılı yazı ile Bilişim Suçlarıyla Mücadele Şube Müdürlüğümüzce yürütülmekte olan ilgili soruşturmaya esas olmak üzere; aşağıda belirtilen IP numarasını kullanan **özel ve tüzel kişilerin telefon, adres ve kimlik** bilgilerine ihtiyaç duyulmaktadır.

IP NUMARASI	TARİH	SAAT
78.179.126.184	10/01/2012	03:05:05

Mevcut bilgilerin tespit edilerek **İlçe Emniyet Müdürlüğüne** gönderilmesi hususunda;

Bilgi ve gereğini arz/rica ederim.

.....
İlçe Emniyet Müdürü
3. Sınıf Emniyet Müdürü

EK:
İlgi sayılı yazı (1 Sayfa)

DAĞITIM :
Gereği :
Türk Telekomünikasyon AŞ'ye

Bilgi:
..... Cumhuriyet Başsavcılığına

İst. Emn. Müd., BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat; T. ÇETİN P.M
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilsim@iem.gov.tr

EK 8

T.C.
KADIKÖY KAYMAKAMLIĞI
İlçe Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.58858-(62217)-**2012/xxxx** .../01/2013

Konu : Bilgi ve Belge Talebi

VODAFONE NET İLETİŞİM HİZMETLERİ AŞ'YE

Ünalan Mah. Ayazma Cad. Çamlıca İş Merkezi B.Blok
Üsküdar/İSTANBUL

İlgi : İstanbul Cumhuriyet Başsavcılığının .../.../2012 tarihli ve 2012/xxxx sayılı yazısı.

İlgi sayılı yazı ile Bilişim Suçlarıyla Mücadele Şube Müdürlüğümüzce yürütülmekte olan ilgili soruşturmaya esas olmak üzere; aşağıda belirtilen IP numarasını kullanan **özel ve tüzel kişilerin telefon, adres ve kimlik** bilgilerine ihtiyaç duyulmaktadır.

IP NUMARASI	TARİH	SAAT
188.3.6.48	19/08/2012	01:38:00

Mevcut bilgilerin tespit edilerek **İlçe Emniyet Müdürlüğüne** gönderilmesi hususunda;
Bilgi ve gereğini arz/rica ederim.

....
İlçe Emniyet Müdürü
3. Sınıf Emniyet Müdürü

EK:
İlgi sayılı yazı (1 Sayfa)

DAĞITIM :
Gereği :
Vodafone Net İletişim Hizmetleri AŞ'ye

Bilgi:
İstanbul Cumhuriyet Başsavcılığına

İst. Emn. Müd. BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat: T. ÇETİN P.M.
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@iem.gov.tr

T.C.
İSTANBUL VALİLİĞİ
İl Emniyet Müdürlüğü

K-Q TSE-ISO-EN 9000

Sayı : B.05.1.EGM.4.34.00.11.02/2007(07/Ds.CBS:476)31050-2083 11./08/2007
Konu : Arama ve El Koyma Talebi

BEYOĞLU' CUMHURİYET BAŞSAVCILIĞINA
(SORUŞTURMA NO:2007/17464)

İLGİ : 02.08.2007 tarih ve 2007/17464 Sayılı Soruşturma yazınız,

İlgi sayılı yazınız ile, Müşteki Elektronik ve Tic.A.Ş firmasına ait www. .com, www. .com, ve www. com ısımli web sitelerine yönelik DDOS tekniği kullanılarak yapılan elektronik saldırıyı yapan şahıs yada şahısların tespiti ile ilgili olarak;

S.NO	IP ADRESİ	İLK GÖRÜNDÜĞÜ TARİH	SON GÖRÜNDÜĞÜ TARİH
1	88.247.16.207	2007-07-15 16:16:54.000	2007-07-30 15:03:24.000
2	88.250.4.199	2007-07-17 11:54:36.000	2007-07-30 17:07:55.000
3	88.247.177.193	2007-07-18 14:58:28.000	2007-07-30 14:45:07.000
4	85.105.182.214	2007-07-14 19:55:12.000	2007-07-18 16:44:40.000
5	88.250.225.157	2007-07-14 19:55:13.000	2007-07-26 19:26:05.000
6	88.247.70.165	2007-07-14 19:55:12.000	2007-07-30 19:08:01.000
7	85.105.216.124	2007-07-17 19:38:53.000	2007-07-25 19:59:31.000
8	85.105.120.205	2007-07-15 16:29:46.000	2007-07-26 18:46:40.000
9	81.214.186.89	2007-07-18 14:58:27.000	2007-07-30 18:08:35.000
10	85.98.34.73	2007-07-14 19:55:12.000	2007-07-26 18:50:35.000
11	212.174.195.18	2007-07-17 11:58:33.000	2007-07-30 16:56:19.000
12	212.174.195.17	2007-07-17 11:58:02.000	2007-07-30 16:52:12.000
13	85.99.233.129	2007-07-17 11:54:36.000	2007-07-25 19:16:11.000
14	88.247.50.35	2007-07-16 20:13:00.000	2007-07-30 19:35:09.000

Yukarıda belirtilen IP numaralarını **kullanan şahısın telefon, adres ve kimlik bilgilerinin tespit edilerek,** gelen görevlilerimize elden verilmesi için yazımızın . **Avrupa Yakası Türk Telekom Müdürlüğü Bilişim Ağları Müdürlüğüne** havalesini arz ederim.

Yılmaz AVCU
Asayiş Şube Müdür V
4.Sınıf Emniyet Müdürü

İSTANBUL AVRUPA YAKASI İL TELEKOM MÜDÜRLÜĞÜ
(Bilişim Ağları Müdürlüğü)'ne

İstenilen bilgi ve belgelerin 0212 214 47 00 numaralı telefona İVEDİ faks çekilmesi veya gelen görevliye elden verilmesini rica olunur.

11/08/2007
Bay.ş.f.a... Cumhuriyet Savcısı

TÜRK TELEKOMÜNİKASYON A.Ş.
İST.YAK. İL TELEKOM MÜD.
BİLİŞİM AĞLARI MÜDÜRLÜĞÜ
NO: 212609 DOSYA
TARİH 13/8/2007

08/08/2007 Büro Memuru :M.CENGİZ
10/08/2007 İnt.Bil.Suç.Kıs.A. :A.SAVRAN
10./08/2007 Büro Amir.V. : Y.ERKURT

İstanbul Emn.Md.lüğü Asayiş Şube Müdürlüğü Ar-Ge ve Bilgi İşlem Büro Amirliği Bilişim Suçları Kısmı Gayrettepe
Telefon: (0212) 214 43 96 Faks: (0212) 214 47 00 Ayrıntılı Bilgi : P.M M.CENGİZ
e-posta: bim.asayis@iem.pol.net, ar-ge.asayis@iem.pol.net

T.C.
İSTANBUL
CUMHURİYET BAŞSAVCILIĞI
BİLİŞİM SUÇLARI BÜROSU

Sayı : 2011/188922 **03/12/2012**

TÜRK TELEKOMÜNİKASYON A.Ş
İSTANBUL 1.BÖLGE MÜDÜRLÜĞÜ
(network yönetim sistemleri müdürlüğü)
VEFA BAYIRI SOKAK NO:2 GAYRETTEPE

Ekte gönderilen **yazıda şirketinize ait ip adreslerini kullanan** hattın kurulu bulunduğu adresleri ve kimin adına kayıtlı (tam kimlik kaydı vatandaşlık numaralı) olduğunun savcılığımıza bildirilmesini rica ederim.

HASAN BASRİ ZAMANİS
34163
Cumhuriyet Savcısı

CMK 332 maddesi uyarınca yazımıza on gün içinde cevap verilmesi zorunlu olup, eğer bu süre içinde istenen bilgilerin verilmesi imkansız ise, sebebi ve en geç hangi tarihte cevap verilebileceği aynı süre içinde bildirmelidir. Aksi halde sorumlular hakkında Türk Ceza Kanununun 257 nci maddesine aykırılıktan adli işlem yapılacaktır.

24)Google şirketinden IP nosu kullanıcı açık kimlik ve adresinin sorulması

T.C.
ESKİŞEHİR VALİLİĞİ
Emniyet Müdürlüğü

SAYI : B.05.1.EGM.4.26.00.16.12. ...../.../2008
15111-Bil.Suç.Br.A.1746/07
KONU : IP Numarasının Araştırılması.

ESKİŞEHİR CUMHURİYET BAŞSAVCILIĞINA

İLGİ : 22.05.2007 tarih ve Soruşturma No:2007/..... sayılı yazısı.

İlgi sayılı yazı ekinde KOM Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğine gönderilen Şikayetçi S..... Ç.....'un ifadesinin tetkikinde; Kurucusu olduğu ..... Eğitim Merkezi olarak ..... tarihinde Eskişehir Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesinde Dış Ticaret adı altında bir seminer düzenlediklerini, bu seminerden sonra internet ortamında .....@gmail.com mail hesabından kurumlarına hakaret ve karalama sözleri yazıldığını beyan ettiği görülmüştür.Konuyla ilgili olarak KOM Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğince ilgi sayılı talimat yazınız ekindeki evraklar incelendiğinde ise, söz konusu mail'in header bilgilerinin alınarak IP numarasının tespit edildiği ve Türk Telekom'dan kullanıcısının tespit edilmek istendiği, ancak Türk Telekom'dan alınan yazıda, söz konusu IP numarasının Google şirketine ait IP bloğu içerisinde yer aldığı anlaşılmıştır.Belirtilen ..... numaralı IP numaralı bilgisayar kullanıcısının tespiti için Türk Telekom'dan alınan yazıda belirtilen Google şirketinin Türkiye Ofisine 25.05.2007 tarihinde yazı gönderilmiş, ancak bugüne kadar herhangi bir cevap alınamamıştır.Şubemizce yapılan araştırmada, Google şirketinin hukuki olarak davalarda muhatap olarak ... HUKUK BÜROSU ile anlaşma yaptığı ve google ile ilgili yazışmaların Elig Hukuk Bürosu'yla yapılabileceği anlaşılmıştır.

Bu durumda ekte fotokopileri gönderilen evrakların tetkik edilerek belirtilen tarih ve saat aralığında .....IP numaralı bilgisayar kullanıcısının açık kimlik ve adres bilgilerinin ivedi Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğümüze ait 0-222-330 77 87 nolu faksına gönderilmesi hususunda Elig Hukuk Bürosuna talimat verilmesini arz ederim.

Ayhan GÜLBASAR
KOM Şube Müdür V.
Emniyet Amiri

EKİ: (6) Adet.

HUKUK BÜROSUNA
(Yıldız Mahallesi Citlenbik Sokak No:12)
Beşiktaş 34349 İSTANBUL

İstenen hususların ivedilikle çıkartılarak Eskişehir Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğüne gönderilmesi rica olunur. ..../.../2008

Hasan GÖNEN
Cumhuriyet Savcısı-38780

TELEFON NUMARASINDAN ABONE BİLGİLERİ SORGULAMA

T.C.
BEYKOZ
CUMHURİYET BAŞSAVCILIĞI
HAZIRLIK BÜROSU

Sayı : 2009/4810 **19/11/2009**

TÜRK TELEKOM BAŞ MÜDÜRLÜĞÜNE
ÜSKÜDAR

Cumhuriyet Başsavcılığımızca yürütülmekte bulunulan hazırlık soruşturmasına esas olmak üzere;

0216 464 62 95 nolu telefonun 12/06/2009 tarihi itibariyle abonesinin açık kimlik ve adresinin tespit edilerek C.Başsavcılığımıza bilgi verilmesi rica olunur.

MURAT BULUT 34264
Cumhuriyet Savcısı

İstanbul Anadolu Yakası
İl Telekom Müdürlüğü

Müşteri İlişkileri Müdürlüğü
Acıbadem cad. no:150
Üsküdar 34660 İstanbul
Tel : (0 216) 555 25 41
Faks: (0 216) 428 30 30
www.turktelekom.com.tr

Sayı : TTŞ.4.34.01.01/ 586.000 150748
Konu : Telefon

14 Aralık 2009

CUMHURİYET BAŞSAVCILIĞI
HAZIRLIK BÜROSU
34820-BEYKOZ

İLGİ :**19.11.2009** gün ve **2009-4810** sayılı yazınız.

İlgi yazınızda bahsi geçen **216-464 62 95** nolu telefon
Bostancı KADIKÖY adresinde kurulu iken **21.05.2009** tarihinde iptal edilmiştir.

Abonenin Bab Adı: D.Yeri ve Tar.: 01.01.1926'dır.

Ayrıca,

"Bundan sonraki telefon ve adres bilgisi taleplerinizi, Telekom Müşteri Servisi (TMS) üzerinden tek merkezden verileceğinden, yazımız tarihi itibariyle sözkonusu bilgi taleplerinin ***"Ankara İl Telekom Müdürlüğü Operatörlü Servisler Müdürlüğü Alsancak Sok. B. Blok 5. Kat ULUS/ANKARA*** adresinden talep edilmesi gerekmektedir.

Saygılarımızla.

Hüseyin ÖZGÜL
Uzman

Ali ÖLÇER
Müdür

İstanbul Anadolu Yakası
İl Telekom Müdürlüğü

Pazarlama Müdürlüğü
Acıbadem cad. no:150
Üsküdar 34660 İstanbul
Tel : (0 216) 555 25 41
Faks: (0 216) 428 30 30
www.turktelekom.com.tr

Sayı : TTŞ.4.34.01.01/D:586.000/
Konu : Telefon

14.08.2007 11693

İSTANBUL VALİLİĞİ
EMNİYET MÜDÜRLÜĞÜNE
34668 – İSTANBUL

İLGİ:14.08.2007 gün ve SAYI: B.05.1.EGM.4.34.00.11.2007 / **2083** sayılı yazınız.

İlgi yazınızda bahsi geçen telefon numarası;

0216-305 66 65 nolu telefon adına kayıtlı olup, " Maltepe" adresinde kuruludur. Abonenin Baba Adı: , Ana Adı: , Doğum Yeri ve Tarihi:Bulancak 22.10.1962'dir.

Ayrıca,

*"Bundan sonraki telefon ve adres bilgisi talepleriniz, Telekom Müşteri Servisi **(TMS)** üzerinden tek merkezden verileceğinden, yazımız tarihi itibariyle söz konusu bilgi taleplerinin **" Ankara İl Telekom Müdürlüğü Operatörlü Servisler Müdürlüğü Alsancak Sok. B. Blok 5. Kat ULUS/ANKARA"** adresinden talep edilmesi gerekmektedir.*

Saygılarımızla.

Yıldız ÖZGÜL
Şef

Zeliha ŞİŞMAN
Şef

11)Başkasına ait kredi kartı bilgileriyle internet üzerinden kontür alan kişinin tesbiti (2)

T.C.
ESKİŞEHİR VALİLİĞİ
Emniyet Müdürlüğü

SAYI : B.05.1.EGM.4.26.00.16.12. …../…/2008
15111-Bil.Suç.Br.A.2512/07
KONU : Bilgi Talebi.

CUMHURİYET BAŞSAVCILIĞINA
ESKİŞEHİR

İLGİ : a)27.07.2007 tarih ve Soruşturma No:2007/……. sayılı talimat yazınız.

b)Akbank Eskişehir Şubesine, Vodafone Telekominikasyon A.Ş.'ye ve Elektronik Bilgi İletişim Hizmetleri Reklamcılık ve Ticaret A.Ş.'ye muhatap 06.08.2007 tarih ve 15111-Bil.Suç.Br.A.2512/07 sayılı dağıtımlı yazımız.

İlgi (a) sayılı talimat yazınız ekinde KOM Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğine gönderilen Şikayetçi İ…… T……'ün dilekçesi ve ifadesinin tetkikinde; Akbank'tan almış olduğu ve bazı internet hizmetlerinde kullanmakta olduğu …… …… …… ……. kart numaralı kredi kartına bağlı olan …….. ……. ……. …… numaralı Axess ek kredi kartıyla bilgisi dışında internet üzerinden **10 Haziran 2007 tarihinde Vodafone şirketinden 110 YTL'lik kontör yüklemesi** ve 25 Haziran 2007 tarihinde EBI AŞ İSTTR (www.siberalem.com) isimli şirketten 88,55 YTL'lik 3 aylık abonelik yapıldığını öğrendiğini, bu işlemleri kendisinin yapmadığını, kredi kart bilgilerini çalarak, internetten alış veriş yapan şahıs/şahıslardan davacı olduğunu beyan ettiği görülmüştür.

Konuyla ilgili olarak yapılacak tahkikata esas olmak üzere İlgi (b) sayılı yazımızla Vodafone Telekominikasyon A.Ş.'ye Şikayetçiye ait …….. ….. ……. ……. kart numaralı Axess ek kredi kartıyla 10 Haziran 2007 tarihinde 110 YTL tutarında Vodafone kontör yüklemesi yapılıp yapılmadığı, yapılmış ise hangi IP numaralı bilgisayardan (Tarih, saat ve saniye aralığı ile birlikte) hangi POS cihazından, hangi GSM hat numaralı telefona yüklendiği, hattın kullanıcısının açık kimlik, adres ve telefon bilgileri ile kimlik fotokopisinin çıkartılarak gönderilmesi için yazı gönderilmesine rağmen bu zamana kadar herhangi bir cevap alınamamıştır.

Cevabi yazının bir an önce gönderilmesi hususunda Vodafone Telekominikasyon A.Ş.'ye talimat verilmesini arz ederim.

Ayhan GÜLBASAR
KOM Şube Müdür V.
Emniyet Amiri

VODAFONE TELEKOMİNİKASYON A.Ş.'YE

(Mehmet Akif Mh.İnönü Cd.Star Sk.No:2)
İkitelli 34540 İSTANBUL

Yukarıda istenen hususların ivedilikle çıkartılarak Eskişehir Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğüne gönderilmesi rica olunur. …./…./2008

Ünal DOĞAN-38087
Cumhuriyet Savcısı

TCK. 245 KAPSAMINDA BANKALARA YAZILAN YAZILAR

2)Başkasına ait kredi kartı bilgileri ile internet üzerinden alış veriş yapılması (2)

T.C.
ESKİŞEHİR VALİLİĞİ
Emniyet Müdürlüğü

SAYI : B.05.1.EGM.4.26.00.16.12. ..../.../2008
15111-Bil.Suç.Br.A.267/08
KONU : Bilgi Talebi.

CUMHURİYET BAŞSAVCILIĞINA
ESKİŞEHİR

İLGİ : 15.01.2008 tarih ve Soruşturma No:2008/..... sayılı talimat yazınız.

İlgi sayılı talimat yazınız ekinde KOM Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğine gönderilen T.... ve Z.... oğlu Ç.....-19... doğumlu A.... B.... isimli şahsın dilekçesinin ve ifadesinin tetkikinde; Citibank'tan almış olduğu 4.... 9.... 8.... 0.... numaralı kredi kartını yaklaşık 5-6 aydır kullandığını, limitinin 1.300,00 YTL olduğunu, 07.01.2008 tarihinde kredi kartıyla kontör almak istediğinde limitinin yetersiz olduğunu gördüğünü, bunun üzerine Citibank Eskişehir Şubesine gittiğini ve durumu sorduğunda kredi kartından 560 YTL değerinde Y.... Ticaret Eskişehir'den alış veriş yapıldığını, ayrıca C... S... Petrol'den de 100 YTL'lik alış veriş yapıldığını öğrendiğini, söz konusu alış verişleri kendisinin yapmadığını, kredi kartını kimseye vermediğini, kendisinin dışında hiç kimsenin bu kredi kartını kullanmadığını, bilgisi haricinde kredi kartından alış veriş yapan şahıstan davacı olduğunu beyan ettiği görülmüştür.

Konuyla ilgili olarak yapılacak soruşturmaya esas teşkil etmek üzere;

1.) Şikayetçi A..... B....'a ait Citibank'tan alınma 4.... 9.... 8.... 0.... numaralı kredi kartına ait söz konusu harcamaları gösteren kredi kartı ekstresinin okunaklı bir şekilde çıkartılması,

2.) Belirtilen harcamaların ne şekilde yapıldığı (POS, internet),

3.) İnternet üzerinden yapılmış ise hangi IP numaradan, hangi tarih ve saat aralığında yapıldığı,

4.) POS cihazından yapılmış ise hangi işyerine ait POS cihazından yapıldığı (İşyerlerinin açık ünvan, adres ve telefonları),

5.) Şikayetçinin konuyla ilgili bankaya bir müracaatının olup olmadığı, bulunuyor ise ne gibi bir işlem yapıldığı,

6.) Söz konusu kredi kartının halen kullanımda olup olmadığı, iptal edilip edilmediği,

7.) Şikayetçinin kredi kartını ne zaman aldığı, aldığı tarihten sonraki harcamaların dökümü (Kredi kartı ekstrelerinin hepsinin okunaklı bir şekilde çıkartılması),

8.) Şikayetçinin kredi kartına herhangi bir ek kart verilip verilmediği bilgilerinin çıkartılarak ivedi olarak Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğümüze gönderilmesi için Citibank Eskişehir Şubesine talimat verilmesini arz ederim.

Ayhan GÜLBASAR
KOM Şube Müdür V.
Emniyet Amiri

CITIBANK ESKİŞEHİR ŞUBESİNE

Yukarıda istenen hususların ivedilikle çıkartılarak Eskişehir Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğüne gönderilmesi rica olunur. .../../2008

Hasan GÖNEN
Cumhuriyet Savcısı-38780

3)Başkasına ait kredi kartı bilgileri ile internet üzerinden alış veriş yapılması (3)

T.C.
ESKİŞEHİR VALİLİĞİ
Emniyet Müdürlüğü

SAYI : B.05.1.EGM.4.26.00.16.12. ..../../2008
15111-Bil.Suç.Br.A.2512/07
KONU : Bilgi Talebi.

CUMHURİYET BAŞSAVCILIĞINA
ESKİŞEHİR

İLGİ : 27.07.2007 tarih ve Soruşturma No:2007/..... sayılı talimat yazınız.

İlgi sayılı talimat yazınız ekinde KOM Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğine gönderilen Şikayetçi İ... T...'ün dilekçesi ve ifadesinin tetkikinde; Akbank'tan almış olduğu ve bazı internet hizmetlerinde kullanmakta olduğu kendisine ait 5... 2.... 3.... 5.. kart numaralı Axess kredi kartıyla bilgisi dışında internet üzerinden **10 Haziran 2007 tarihinde Vodafone şirketinden 110 YTL'lik kontör yüklemesi** ve **25 Haziran 2007 tarihinde EBI AŞ İSTTR (www.siberalem.com) adresine ait şirketten 88,55 YTL'lik 3 aylık abonelik yapıldığını öğrendiğini**, bu işlemleri kendisinin yapmadığını, www.siberalem.com isimli site yetkilileriyle yaptığı e-mail görüşmelerinde 88,55 YTL'lik aboneliğin Antalya'da bulunan coolesis rumuzunu kullanan bilgisayar teknisyeni olarak görünen şahıs tarafından yapıldığını öğrendiğini, kredi kart bilgilerini çalarak, internetten alış veriş yapan şahıs/şahıslardan davacı olduğunu beyan ettiği görülmüştür.

Konuyla ilgili olarak yapılacak tahkikata esas olmak üzere;

1.) Şikayetçi H..... ve S..... oğlu 1981 doğumlu İ... T...'e ait 5... 2...3... 5... kart numaralı ek kart verilip verilmediği, asıl kartın kime verildiği, 10 Haziran 2007 ve 25 Haziran 2007 tarihlerinde yapılan harcamaların hangi IP numaralı bilgisayar kullanılarak gerçekleştirildiği (Saat ve saniye bilgileri ile birlikte), konuyla ilgili şikayetçinin müracaatının bulunup bulunmadığı, bulunuyor ise ne gibi bir işlem yapıldığı bilgileri, şikayetçinin kredi kartına ait hesap ekstresi ile olayın çözümüne yarayacak her türlü detay bilgisinin çıkartılması hususunda ***Akbank Eskişehir Şubesine,*** (Şikayetçinin hesabı başka bir Akbank Şubesinde olsa bile ilgili Şube ile irtibata geçilerek istenen hususların çıkartılması),

2.) Şikayetçiye ait 5... 2... 3...5423 kart numaralı Axess kredi kartıyla 10 Haziran 2007 tarihinde 110 YTL tutarında Vodafone kontör yüklemesi yapılıp yapılmadığı, yapılmış ise hangi IP numaralı bilgisayardan (Tarih, saat ve saniye aralığı ile birlikte) hangi POS cihazından, hangi GSM hat numaralı telefona yüklendiği, hattın kullanıcısının açık kimlik, adres ve telefon bilgileri ile kimlik fotokopisinin çıkartılarak gönderilmesi için ***Vodafone Telekominikasyon A.Ş.'ye,***

3.) Halen Elektronik Bilgi İletişim Hizmetleri Reklamcılık ve Ticaret A.Ş.'ye bağlı olarak faaliyet gösterdiği anlaşılan www.siberalem.com isimli internet sitesine, şikayetçiye ait 5.... 2.... 3.... 5... kart numaralı Axess kredi kartıyla 88,55 YTL karşılığında 3 aylık abonelik yaptığı beyan edilen şahsın, abone numarasının, açık kimlik, adres ve telefon bilgilerinin, şahsın ilgili siteye bağlandığı bilgisayarın IP numarasının (Tarih, saat ve saniye aralığı ile

birlikte) ve her türlü detay bilgisinin çıkartılarak gönderilmesi hususunda ***Elektronik Bilgi İletişim Hizmetleri Reklamcılık ve Ticaret A.Ş.***'ye talimat verilmesini arz ederim.

Ayhan GÜLBASAR
KOM Şube Müdür V.
Emniyet Amiri

AKBANK ESKİŞEHİR ŞUBESİNE

VODAFONE TELEKOMİNİKASYON A.Ş.'YE

(Mehmet Akif Mh.İnönü Cd.Star Sk.No:2)
İkitelli 34540 İSTANBUL

VE

ELEKTRONİK BİLGİ İLETİŞİM HİZMETLERİ REKLAMCILIK VE TİCARET A.Ş.'YE

(Yurt Sokak No:29)

Çağlayan / İSTANBUL

Yukarıda istenen hususların ivedilikle çıkartılarak Eskişehir Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğüne gönderilmesi rica olunur. ../.../2008

Hasan GÖNEN
Cumhuriyet Savcısı-38780

10)Başkasına ait kredi kartı bilgileriyle internet üzerinden kontür alan kişinin tesbiti (1)

T.C.
ESKİŞEHİR VALİLİĞİ
Emniyet Müdürlüğü

SAYI : B.05.1.EGM.4.26.00.16.12. ..../..../2008
15111-Bil.Suç.Br.A.2305/07
KONU : Bilgi Talebi.

CUMHURİYET BAŞSAVCILIĞINA
ESKİŞEHİR

İLGİ : 04.07.2007 tarih ve Soruşturma No:2007/..... sayılı talimat yazınız.

İlgi sayılı talimat yazınız ekinde KOM Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğine gönderilen V.... B.... isimli şahsın dilekçesi ve ifadesinin tetkikinde; Adına kayıtlı bulunan 4.... 0... 2.... 8.... nolu Akbank Axess kredi kartından bilgisi olmadan 220 YTL değerinde Vodafone kontör alış verişi yapıldığını, bu bilgiyi 14.06.2007 tarihinde ilgili bankaya ne kadar borcu olduğunu sormaya gittiğinde öğrendiğini, bankadan almış olduğu belgede söz konusu kredi kartı ile İstanbul'dan 220 YTL değerinde kontör alış verişi yapıldığını gördüğünü, bu işlemin internet bankacılığı ile yapıldığını öğrendiğini, kendisinin internet bankacılığını kullanmadığını beyan etmiştir.

KOM Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğince yapılacak soruşturmaya esas teşkil etmek üzere;

1.) Şikayetçiye ait 4.... 0.... 2... 8.... nolu Akbank Axess kredi kartı ile internet üzerinden 220 YTL değerinde Vodafone kontör alımı yapılıp yapılmadığı,

2.) Yapılmış ise, söz konusu harcamanın hangi tarih ve saatte hangi IP numaralı bilgisayar kullanılarak (Tarih, saat, dakika ve saniye aralığı ile birlikte), hangi işyerinden yapıldığı, işyerinin Akbank'la anlaşmalı olup olmadığı, anlaşmalıysa açık adresinin bildirilmesi,

3.) Yapılan harcamanın hangi internet sitesinden yapıldığı, alınan Vodafone kontör kartının kontrol numarasının veya şifresinin bulunup bulunmadığı,

4.) Şikayetçinin konuyla ilgili Akbank'a herhangi bir müracaatının bulunup bulunmadığı,

5.) Şikayetçinin müracaatının olması durumunda ne gibi bir işlem yapıldığı,

6.) Şikayetçinin söz konusu kredi kartının halen aktif olup olmadığı ile,

7.) Şikayetçinin kredi kartına ait 14.06.2007 tarihli ekstresinin çıkartılarak ivedi Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğümüze gönderilmesi için Akbank Eskişehir Şubesine (Eğer şikayetçinin kredi kartı başka bir Akbank Şubesinden alınmış ise,

ilgili Banka Şubesi ile irtibata geçilerek istenen hususların gönderilmesi) talimat verilmesini arz ederim.

Ayhan GÜLBASAR
KOM Şube Müdür V.
Emniyet Amiri

AKBANK ESKİŞEHİR ŞUBESİNE

Yukarıda istenen hususların ivedilikle çıkartılarak Eskişehir Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğüne gönderilmesi rica olunur. …./…./2008

Ünal DOĞAN- 38087
Cumhuriyet Savcısı

11)Başkasına ait kredi kartı bilgileriyle internet üzerinden kontür alan kişinin tesbiti (2)

T.C.
ESKİŞEHİR VALİLİĞİ
Emniyet Müdürlüğü

SAYI : B.05.1.EGM.4.26.00.16.12. …../…/2008
15111-Bil.Suç.Br.A.2512/07
KONU : Bilgi Talebi.

CUMHURİYET BAŞSAVCILIĞINA
ESKİŞEHİR

İLGİ : a)27.07.2007 tarih ve Soruşturma No:2007/..... sayılı talimat yazınız.

b)Akbank Eskişehir Şubesine, Vodafone Telekominikasyon A.Ş.'ye ve Elektronik Bilgi İletişim Hizmetleri Reklamcılık ve Ticaret A.Ş.'ye muhatap 06.08.2007 tarih ve 15111-Bil.Suç.Br.A.2512/07 sayılı dağıtımlı yazımız.

İlgi (a) sayılı talimat yazınız ekinde KOM Şube Müdürlüğümüz Bilişim Suçları Büro Amirliğine gönderilen Şikayetçi İ..... T.....'ün dilekçesi ve ifadesinin tetkikinde; Akbank'tan almış olduğu ve bazı internet hizmetlerinde kullanmakta olduğu .... kart numaralı kredi kartına bağlı olan .... numaralı Axess ek kredi kartıyla bilgisi dışında internet üzerinden **10 Haziran 2007 tarihinde Vodafone şirketinden 110 YTL'lik kontör yüklemesi** ve 25 Haziran 2007 tarihinde EBI AŞ İSTTR (www.siberalem.com) isimli şirketten 88,55 YTL'lik 3 aylık abonelik yapıldığını öğrendiğini, bu işlemleri kendisinin yapmadığını, kredi kart bilgilerini çalarak, internetten alış veriş yapan şahıs/şahıslardan davacı olduğunu beyan ettiği görülmüştür.

Konuyla ilgili olarak yapılacak tahkikata esas olmak üzere İlgi (b) sayılı yazımızla Vodafone Telekominikasyon A.Ş.'ye Şikayetçiye ait .... kart numaralı Axess ek kredi kartıyla 10 Haziran 2007 tarihinde 110 YTL tutarında Vodafone kontör yüklemesi yapılıp yapılmadığı, yapılmış ise hangi IP numaralı bilgisayardan (Tarih, saat ve saniye aralığı ile birlikte) hangi POS cihazından, hangi GSM hat numaralı telefona yüklendiği, hattın kullanıcısının açık kimlik, adres ve telefon bilgileri ile kimlik fotokopisinin çıkartılarak gönderilmesi için yazı gönderilmesine rağmen bu zamana kadar herhangi bir cevap alınamamıştır.

Cevabi yazının bir an önce gönderilmesi hususunda Vodafone Telekominikasyon A.Ş.'ye talimat verilmesini arz ederim.

Ayhan GÜLBASAR
KOM Şube Müdür V.
Emniyet Amiri

VODAFONE TELEKOMİNİKASYON A.Ş.'YE
(Mehmet Akif Mh.İnönü Cd.Star Sk.No:2)
İkitelli 34540 İSTANBUL

Yukarıda istenen hususların ivedilikle çıkartılarak Eskişehir Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğüne gönderilmesi rica olunur. …./…./2008

Ünal DOĞAN-38087
Cumhuriyet Savcısı

MICROSOFT TELEKOM IP NUMARALARI ŞAHIS TESPİTİ

Ek 3

HUKUK BÜROSU

Bilgi Sa.Su.Ge. Kan.

İSTANBUL VALİLİĞİ
EMNİYET MÜDÜRLÜĞÜ'NE

2012

Sayı:

Konu: Bilgi ve Belge Talebi

İlgi: a) C. Başsavcılığı'nın 11.01.2012 tarih ve sayılı yazısı,

b) tarihli yazınız.

Dilekçe Sunan Microsoft Corporation

Vekilleri Av. Metin - Av. Deniz
Büyükdere Cad. No: 151, B Blok, D. 32, Zincirlikuyu, İstanbul

Konu Müvekkile gönderilen 03.07.2012 tarihli yazınıza karşı cevaplarımızdır.

AÇIKLAMALAR

1. Müdürlüğünüzün ilgi yazısı ile soruşturmaya konu olan ve adreslerine erişim neticesinde oluşan IP bilgilerinin tarafınıza gönderilmesi talep edilmişti.

2. adresine erişim neticesinde oluşan IP bilgileri aşağıda sunulmaktadır. **Aşağıda belirtilen tarihler Amerikan sistemine göre yazılmış olup, ay/gün/yıl olarak belirtilmiştir.**

IP Bilgileri	Tarih ve Zaman (Amerika Pasifik Zamanı)	Onay Durumu Pass. Fail
78.179.126.184	1/9/2012 05:05:05 PM (PST)	pass

Örnek olarak yukarıda belirtilen IP numarasını Türkiye saatine çevirelim:

Zaman dilimi PST yani Pasifik Standart Zaman dilimidir. PST zaman dilimi ise Türkiye zaman diliminden 10 Saat geridedir, bu da demektir ki PST zaman dilimine göre verilen 05:05:05 PM saatine 10 saat eklememiz gerekmektedir. PM dediği öğleden sonra olduğu için saatimiz 24 saat diliminde 17:05:05 olacak ve bu saate 10 saat eklediğimizde saatimizin Türkiye deki karşılığı 03:05:05 olacaktır. **Ancak burada dikkat edilmesi geregen husus ise saatimiz bir sonraki güne atladığı için tarih de bir sonraki güne devredicek yani tarihimiz PST zamanında 09/01/2012 iken Türkiye zamanında ise 10/01/2012 olacaktır.**

Saat çevirisi

tel: 0 212 356 01 13 - 0 212 356 01 14 | fax: 0 212 356 01 09 | web: www.calis.av.tr | e-mail: metin@calis.a..tr

Türk Telekominikasyon A.Ş.
İst.Yaks.İl Telekom Müdürlüğü

Bilişim Ağları Müdürlüğü
Vefa bayırı sok.No:2 Gayrettepe
34349-İSTANBUL
Tel:0212 288 80 47
Faks:0212 288 21 34
www.turktelekom.com.tr

SAYI:T.T.Ş.4.34.02.02 / 213557
KONU: Kimlik ve Adres Tespiti

13 Ağustos 2007

İSTANBUL İL EMNİYET MÜDÜRLÜĞÜNE
Asayiş Şube Müdürlüğü Arge Birim Amirliği
Gayrettepe/İstanbul

İlgi: **11.08.2007** gün ve **B.05.1.EGM.4.34.00.11.02.2007(07/Ds.CBS:476) 31050-2083** No'lu yazınız.

İlgi yazı ile kullanım bilgileri talep edilen IP numaraları **EK**'te bilgileri verilen müşteriler (ADSL müşterisi) hesapları adına kullanılmıştır

.

Söz konusu tespit talebine ait mahkeme kararının Ceza Muhakemeleri Kanununun 135inci maddesinin 1inci fıkrasına göre en geç 24 saat içerisinde hakim tarafından onaylanarak tarafımıza iletilmesi gerekmektedir

Bilgilerinizi ve gereğini arz ederim.

13/08

Sırrı DURUKANOĞLU
Bilişim Ağları Müdürü

Rüstem BAYRAKTAR Tek Uzm.

Ömer ÇELİKÖRS Şef Müh.

13/08

EK:2 Sayfa

MÜŞTERİ BİLGİLERİ:

Ip Numarası:	**88.247.16.207 STATİK IP**
Ad Soyad:	TİC. SAN.
Adres:	pk:05000 ORGANİZE SAN.BÖLGESİ MERKEZ AMASYA
Telefon:	+90 (358) 2735409
Bağlandığı Tarih ve Saat:	12-07-2007 13:56:36.0
Bağlantının Kesildiği Tarih ve Saat:	19-07-2007 15:53:27.0

Ip Numarası:	**88.250.4.199 STATİK IP**
Ad Soyad:	TİC LTD ŞTİ
Adres:	DEMİRLİBAHÇE MH PLEVNE CD no:30pk:06340 DEMİRLİBAHÇE MAMAK ANKARA
Telefon:	312 3636861
Bağlandığı Tarih ve Saat:	17.07.2007 10:22:55
Bağlantının Kesildiği Tarih ve Saat:	18.07.2007 16:25:13

Ip Numarası:	**88.247.177.193 STATİK IP**
Ad Soyad:	
Adres:	BURSA 2.MURAT C.
Telefon:	+90 (224) 2205566
Bağlandığı Tarih ve Saat:	04-07-2007 20:16:34.0
Bağlantının Kesildiği Tarih ve Saat:	18-07-2007 15:34:35.0

Ip Numarası:	**85.105.182.214 STATİK IP**
Ad Soyad:	TİC LTD.ŞTİ
Adres:	pk:16140 NİLÜFER BURSA
Telefon:	+90 (224) 2416708
Bağlandığı Tarih ve Saat:	13-07-2007 16:25:46.0
Bağlantının Kesildiği Tarih ve Saat:	14-07-2007 19:57:21.0

Ip Numarası:	**88.250.225.157 STATİK IP**
Ad Soyad:	
Adres:	MERKEZ KUTAHYA
Telefon:	+90 (274) 2169990
Bağlandığı Tarih ve Saat:	14-07-2007 09:56:18.0
Bağlantının Kesildiği Tarih ve Saat:	14-07-2007 22:18:34.0

Ip Numarası:	**88.247.70.165 STATİK IP**
Ad Soyad:	
Adres:	pk:26170 MERKEZ ESKISEHIR
Telefon:	+90 (222) 3224336
Bağlandığı Tarih ve Saat:	13-07-2007 09:16:50.0
Bağlantının Kesildiği Tarih ve Saat:	15-07-2007 16:40:20.0

Ip Numarası:	**85.105.216.124 STATİK IP**
Ad Soyad:	
Adres:	no:6 pk:42050 KARATAY KARATAY KONYA
Telefon:	+90 (332) 3423540
Bağlandığı Tarih ve Saat:	17-07-2007 11:14:55.0
Bağlantının Kesildiği Tarih ve Saat:	17-07-2007 20:24:21.0

Ip Numarası:	**85.105.120.205 STATİK IP**
Ad Soyad:	
Adres:	laire:A pk:06570 MALTEPE ÇANKAYA ANKARA
Telefon:	+90 (312) 2316116
Bağlandığı Tarih ve Saat:	15-07-2007 07:36:54.0
Bağlantının Kesildiği Tarih ve Saat:	15-07-2007 23:28:25.0

Ip Numarası:	**81.214.186.89 STATİK IP**
Ad Soyad:	BİLİŞİM AĞLAR MÜDÜRLÜĞÜBİLİŞİM AĞLAR MÜDÜRLÜĞÜ
Adres:	YENİŞEHİR MARDİN YOLU no:1kat:1 pk:63300 YENİŞEHİR MERKEZ SANLIURFA
Telefon:	+90 (414) 3151883
Bağlandığı Tarih ve Saat:	17-07-2007 09:57:41
Bağlantının Kesildiği Tarih ve Saat:	18-07-2007 15:00:20

Ip Numarası:	**85.98.34.73 STATİK IP**
Ad Soyad:	LTD.ŞTİ
Adres:	. pk:54600 MERKEZ SAPANCA SAKARYA
Telefon:	+90 (264) 5820738
Bağlandığı Tarih ve Saat:	14-07-2007 18:35:06
Bağlantının Kesildiği Tarih ve Saat:	14-07-2007 19:55:13

Ip Numarası:	**85.99.233.129 STATİK IP**
Ad Soyad:	
Adres:	no:50kat:00000 daire:00000 pk:034775 ÜMRANİYE ISTANBUL-AND
Telefon:	+90 (216) 5405046
Bağlandığı Tarih ve Saat:	17-07-2007 07:55:24.0
Bağlantının Kesildiği Tarih ve Saat:	17-07-2007 11:56:38.0

Ip Numarası:	**88.247.50.35 STATİK IP**
Ad Soyad:	
Adres:	pk:33110 MERKEZ YENİŞEHİR MERSIN
Telefon:	+90 (324) 3282875
Bağlandığı Tarih ve Saat:	16-07-2007 20:12:18.0
Bağlantının Kesildiği Tarih ve Saat:	16-07-2007 20:16:54.0

212.174.195.17, 212.174.195.18 IP numaraları şirketimize ait değildir. RIPE'ten alınan bilgileri aşağıdadır.

```
% Information related to '212.174.195.16 - 212.174.195.31'
inetnum:        212.174.195.16 - 212.174.195.31
netname:        BELBIM
descr:          Belbim A.S.
descr:          Istanbul belediyeleri Bilgi Islem A.S.
country:        TR
admin-c:        RB19352-RIPE
tech-c:         RB19352-RIPE
status:         ASSIGNED PA Definition
mnt-by:         AS9121-MNT
source:         RIPE # Filtered
person:         Ruhi Bayraktar
address:        Bulgurlu Mah. Libadiye Cad.
address:        No:27 Usküdar
address:        Istanbul
phone:          +90 2165217090
fax-no:         +90 2165217374
```

İstanbul I Bölge Müdürlüğü
Network Yönetim Sistemleri Müdürlüğü

Türk Telekomünikasyon A.Ş.
Yıldız Posta Cd. Vefa Bayırı Sk: No:2 34349 Gayrettepe /İstanbul
Tel: (0212) 288 80 47 Faks: (0212) 288 21 34

444 1 444 TURKTELEKOM.COM.TR

SAYI: T.T.Y.G.BL01.34.01.04/575 340624 10 Aralık 2012
KONU: Bilgi Talebi

HUKUK MÜDÜRLÜĞÜNE

İlgi: İstanbul Cumhuriyet Başsavcılığının 03.12.2012 tarih ve 2011/188922 sayılı yazısı

İstanbul Cumhuriyet Başsavcılığının 03.12.2012 tarih ve 2011/188922 sayılı yazının müzekkeresine verilecek cevap EK'de belirtilmiştir.

Bilgilerinizi ve gereğini arz ederim.

[illegible] TERGUT

EK:1 Sayfa

TÜRK TELEKOMÜNİKASYON A.Ş.
İSTANBUL-I BÖLGE MÜDÜRLÜĞÜ
HUKUK MÜDÜRLÜĞÜ 340624
Geliş Tarihi :
Geliş No : 265
Dosya No :
11 Aralık 2012

BAĞLANTI BİLGİLERİ:

85.102.51.187 / 85.96.35.69 / 85.101.2.95 / 88.233.242.110 / 88.233.242.110 / 85.96.237.87 / 88.235.88.220 / 85.102.52.82 / 88.233.240.227 / 88.233.13.69 / 85.101.7.143 / 88.235.32.51 / 88.233.245.93 / 85.101.21.222 / 88.233.244.71 / 85.96.58.35 / 85.101.7.99 / 85.101.0.169 / 88.233.247.27 / 81.214.7.79 / 85.101.20.79 / 88.234.189.118 / 85.101.7.1 / 85.101.221.0 / 88.235.25.195 / 85.101.2.247 / 85.96.58.116 / 88.233.114.31 / 85.102.134.23 / 85.102.49.172/ 85.102.188.135 / 88.233.10.32 / 85.96.113.151 / 85.97.45.89 / 85.97.148.108 / 88.234.188.180 / 85.102.185.87 / 85.96.26.6 / 85.97.0.74 / 88.234.121.99 / 88.235.31.250 / 88.234.11.254 / 85.102.205.96 / 212.156.165.168 / 85.97.71.218 / 85.97.45.126 / 85.101.22.66 IP numaraları belirtilen tarih ve saatlerde aşağıdaki müşterimiz tarafından kullanılmıştır.

Ip Numarası:	
Ad Soyad:	SAN TİC LTD
Adres:	PK:34384 BEYOGLU ISTANBUL_AVR
Telefon:	212 -361 80 60
Bağlandığı Tarih ve Saat:	
Bağlantının Kesildiği Tarih ve Saat:	
Müşteri T.C Kimlik No:	

ARAMA EL KOYMA TALEBİ

T.C
İSTANBUL VALİLİĞİ
Emniyet Müdürlüğü

07/590 muh.

K-Q TSE-ISO-EN 9000

Sayı : B.05.1.EGM.4.34.00.11.02.2007/(07- Ds.CBS:476)31050-2083 15./08/2007

Konu : Arama İzni, İnceleme ve El Koyma İzni

KARTAL CUMHURİYET BAŞSAVCILIĞINA

İlgi : (a) Beyoğlu C.Başsavcılığının 02.08.2007 tarih ve 2007/17464 soruşturma sayılı yazısı,
(b) İstanbul Anadolu Yakası Türk Telekom Müdürlüğünün 14.08.2007tarihli yazısı,

Beyoğlu Cumhuriyet Başsavcılığının ilgi (a) sayılı yazısı ile yürütülen soruşturma gereği; müşteki I .. Tic. A.Ş.' vekili tarafından verilen şikayet dilekçesine istinaden şirkete ait www. ....com isimli internet sitesine internet üzerinden DDOS atak denilen sanal saldırı yapmak suretiyle bilişim sisteminin işleyişini engelleyen, sistemi işlemez hale getiren ve sisteme kayıtlı üyelerin sisteme girişlerini engelleyen bilgisayar kullanıcılarının açık kimlik ve adres bilgilerinin tespit edilmesi istenmiştir.

DDOS atağı, bir bilişim sistemine sistemin kaldırabileceğinin çok üzerinde hizmet isteği gönderi[illegible]si ve bu nedenle ana sistemin gelen bu hizmet isteklerine cevap verememesi olayıdır.

Şikayetçi firmanın şikayet dilekçelerinde belirtmiş oldukları Şüpheli Batuhan isimli şahıs hakkında yapılan araştırmada şahsın 0216 [illegible] numaralı sabit telefon hattını kullandığının belirlenmesi üzerine bu hattı kullanan abonenin açık kimlik ve adres bilgilerinin belirlenmesi için İstanbul Anadolu Yakası Türk Telekom Müdürlüğü ile gerekli yazışmalar yapılmış ve ilgi (b) sayılı cevap yazılarına kayden abone bilgisi aşağıdaki tablo şekliyle tespit edilmiştir.

S.N.	TELEFON NO	ABONE ADI	ADRES
1	021		Sk. No: Daire: Kat: **Maltepe - İSTANBUL**

Soruşturama dosyasının soruşturulması, olayı gerçekleştiren şahıslar hakkında gerekli yasal işlemlerin yapılabilmesi için başka suretle delil etme imkanı bulunmadığından dolayı;

1- Yukarıda tabloda belirtilen adreste suç kanıtlarının ele geçirilmesi için CMK 116. maddesi uyarınca **ARAMA YAPILMASI,**
2- Arama sonucu ele geçirilecek bilgisayar(ların) programları ile bilgisayar kütüklerinde ar[illegible]a yapılmasına , suç unsuru bulunması halinde bilgisayar kayıtlarından kopya çıkartılmasına, bu kayıtların çözülerek metin haline getirilmesi için CMK 134/1. maddesi uyarınca **İZİN VERİLMESİ,**
3- Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için CMK 134/2. maddesi uyarınca **EL KONULMASI** için,

İlgili mahkemeden karar aldırılmasını arz ederim.

Mustafa KÖSE
Asayiş Şube Müdürü
3.Sınıf Emniyet Müdürü

EKİ : Soruşturma Evrakları(... sayfa)

15/08/2007 Büro Memuru :E.KUVETLİ
15/08/2007 İnt.Bil.Suç.Kıs.A.:D.AY

Asayiş Şube Müdürlüğü Arge Büro Amirliği İnternet ve Bilişim Suçları Kısmı Gayrettepe/İstanbul
Telefon : 0212 214 43 96 Fax : 0212 214 47 00 Ayrıntılı Bilgi İçin; Polis Memuru EYÜP KUVETLİ

EK 9

T.C.
KADIKÖY KAYMAKAMLIĞI
İlçe Emniyet Müdürlüğü

Sayı :B.05.1.EGM.4.34-58858-(62217)-2012/..... .../10/2012

Konu :Arama. El Koyma ve İnceleme Kararı Talebi

..... CUMHURİYET BAŞSAVCILIĞINA
(Hazırlık Bürosu-Soruşturma No: 2012/xxxx)

İlgi : a) İstanbul Cumhuriyet Başsavcılığının .../.../2012 tarihli ve 2012/xxxx sayılı yazısı,
b) Turkcell İletişim Hizmetleri AŞ' nin .../.../2012 tarihli yazısı,

İlgi (a) sayılı yazı ile İlçe Emniyet Müdürlüğümüzce yürütülmekte olan bir tahkikata esas olmak üzere; müşteki ..... Bildirilerek gerekli çalışmaların yapılması istenmektedir.

İlgi (a) sayılı İstanbul Cumhuriyet Başsavcılığınca yürütülen soruşturmaya esas olmak üzere, ilgi (a) sayılı yazı ile bildirilen abc@hotmail.com isimli e posta adresini kullanan şahıs yada şahısların, e posta adresine erişim sağlarken kullanmış olduğu IP numaraları tarih ve saat bilgileriyle Turkcell İletişim Hizmetleri AŞ' ye sorularak bilgi ve belge talep edilmiştir.

İlgi (b) sayılı Turkcell İletişim Hizmetleri AŞ 'den alınan cevabi yazıda kullanıcı bilgileri sorgulanan IP numaralarının soruşturma evrakında ismi geçen, Kadıköy Mah Kadıköy Sok. No:1/5 Kadıköy/İSTANBUL adresinde ikamet eden.....isimli şahsın kullanmış olduğu **0500 000 00 00**nolu telefondan erişim sağlandığı bildirilmiştir. .

Yapılan çalışmalarda şüpheli .....İsimli şahsın**"Kadıköy Mah. Kadıköy Sok. No:1/5 Kadıköy/İSTANBUL"** sayılı adreste ikamet edip etmediğini teyit etmek maksadı ile adrese gidilmiş, adres çevresinde yapılan araştırmalarda şüpheli şahsın **"Kadıköy Mah. Kadıköy Sok. No:1/5 Kadıköy/İSTANBUL"** adresinde ikamet ettiği hazırlanan tutanakta belirtilmiştir.

İlgi (a) sayılı soruşturmaya istinaden .....isimli şahıs için tespit edilen **"Kadıköy Mah. Kadıköy Sok. No:1/5 Kadıköy/İSTANBUL"** sayılı adreste, gerçekleşen suça ait delillerin tespit edilmesi ve suç unsurlarının ele geçirilmesi için:

- **5271 Sayılı Yasanın 116. ve 117. Maddeleri gereğince ARAMA YAPILMASINA,**

İst. Emn. Müd., BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat: T. ÇETİN P.M
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@iem.gov.tr

- Arama neticesi elde edilecek suç unsuru materyaller hakkında **5271 Sayılı Yasanın 127. Maddesi** gereğince **EL KONULMASINA,**

- Adreste bulunan bilgisayar kasası, harddisk, laptop ve modem gibi materyallerin incelenmesi, arama yapılacak adreste mümkün değilse kopyası alınmak üzere geçici olarak tarafımızdan el konulması ve Bilişim Suçlarıyla Mücadele Şube Müdürlüğümüzce gerekli araştırma ve incelemenin yapılabilmesi için **5271 Sayılı Yasanın 134. Maddesi** ve **Adli ve Önleme Arama Yönetmeliğinin 17. Maddesi** gereğince **İNCELEME YETKİSİ** verilmesine.

Soruşturmanın sağlıklı bir şekilde sonlandırılabilmesi için karar tarihinden itibaren 3 **(üç) gün içerisinde gündüzleyin bir defaya mahsus olmak üzere ARAMA, EL KOYMA ve İNCELEME KARARI** alınması noktasında ön olmanız hususunda:

Gereğini arz ederim.

.....
İlçe Emniyet Müdürü
3. Sınıf Emniyet Müdürü

EKLER:
1- İlgi (a)sayılı yazı (... Sayfa)
2- İlgi (b) sayılı yazı (... Sayfa)

İst. Emn. Müd., BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat: F. ÇETİN P.M.
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@iem.gov.tr

SULH MAHKEMESİ ARAMA KARARI

TÜRK MİLLETİADINA

T.C.

KARTAL

2.SULH CEZA MAHKEMESİ

D.İŞ NO : 2007/ 1860

ARAMA KARARI

HAKİM : LATİF KADİR KAYA 36860

KATİP : BEDRİYE GENÇ 760

TALEP EDEN : İSTANBUL VALİLİĞİ EMNİYET MÜDÜRLÜĞÜ.
15.08.2007- B.05.1.EGM.4..34.00.11.12 -2007/ (07-Ds.CBS 476)
(Kartal C.Başsavcılığı 15.08.2007 tarih ve 2007/ 590 sor.muh)

TALEP TAR.VE SAYISI : 15.08.2007

KARAR TA. : 15.08.2007

Kartal C.Başsavcılığının yukarıda tarih ve sayılı talepnamesi ile arama kararı verilmesi talep olunmuştur.

Soruşturma evrakının içeriğine göre,suç delillerinin elde edilebileceği ve şüphelinin tespit olunabileceği hususunda makul şüphe bulunduğundan ve talepteki gerekçe yerinde görüldüğünden kabulü gerekmiştir.

KARAR :

1-**TALEBİN KABULUNE**.

Aşağıda belirtilen fiil nedeni ile,suçun tespiti,suç delillerinin elde edilebilmesi ve şüphelinin yakalanabilmesi bakımından;

Aşağıda belirtilen yerde ve belirlenen süre içinde;

KOLLUK GÜÇLERİNCE GÜNDÜZLEYİN BİR DEFAYA MAHSUS OLMAK ÜZERE ARAMA YAPILMASINA.

a-)Yapılacak aramada Anayasa tarafından güvence alınan kişi hak ve hürriyetlerinin gözetilmesine,aramanın 5271 Sayılı Kanunun 119/3-4 maddesine ve Adli-İdari Aramalar yönetmeliğine uygun şekilde yapılmasına.

b-)Arama işlemi öncesi,mahkememiz kararının aramayı yapan görevliler tarafından arama yapılacak yerin sahip veya yetkilisine tebliğ olunmasına.

Arama başlangıcının ve bitiminin tutanakla tespitine.

2-Arama sonucu ele geçirilecek bilgisayar veya bilgisayarların programları ile **BİLGİSAYAR KÜTÜKLERİNDE ARAMA YAPILMASINA.**

Suç unsuru bulunması halinde **BİLGİSAYAR KAYITLARINDAN KOPYA ÇIKARILMASINA**

BU KAYITLARIN ÇÖZÜLEREK METİN HALE GETİRİLMESİ İÇİN CMK.134/1 MADDESİ UYARINCA İZİN VERİLMESİNE

2-Arama sonucu suçun ispatına yarayacak yarayacak belge,kağıt,eşya veya taşınması ve bulundurulması bizatihi suç teşkil eden eşya elde edilmesi halinde **EL KONULMASINA**.

3- Belirtilen fiil nedeniyle yapılan aramada ele geçen,suç delili teşkil eden eşyaya **EL KONULMA İŞLEMİNİN ONANMASINA** .

4-El konulan eşya üzerinde C.Başsavcılığınca gerekmesi halinde **BİLİRKİŞİ İNCELEMESİ YAPTIRILABİLMESİNA.**

5-El konulan eşyanın **ADLİ EMANETE ALINMASINA** veya C.savcılığınca belirlenecek uygun yerde **MUHAFAZA ALTINA ALINMASINA**

6-El koyma işleminin yapılması halinde,eşyaya el konulduğu tarihten itibaren 15 gün içerisinde hak sahiplerinin yetkili mahkemede **ŞİKAYET VE BAŞVURUDA BULUNABİLMELERİNE**.

Dair,ilgililerin kararı öğrendikleri günden itibaren yedi gün içerisinde mahkememize verecekleri dilekçe ile veya tutanağa geçirilmek koşulu ile mahkememiz zabıt katibine beyanda bulunmak sureti ile itirazı kabil olmak üzere,5271 Sayılı Kanunun 119-127.maddeleri gereğince,evrak üzerinden karar verildi.15.08.2007

ARAMA KARARINA NEDEN OLAN FİİL : İLETİŞİM SİSTEMİNİ ENGELLEME,BOZMA,VERİLERİ YOK ETME

ARAMANIN YAPILACAĞI YER :MALTEPE,... SOKAK.N.1 SAYILI YERDE VE MÜŞTEMİLATINDA

ARAMANIN YAPILACAĞI SÜRE : Karar tarihinden itibaren 3 gün içerisinde,C.Başsavcılığınca uygun görülecek günde gündüz vakitlerinde bir defaya mahsus olmak üzere.

Katip

Hakim 36860

EL KONULAN EŞYALARIN İNCELENMESİ İÇİN HARDDİSK TALEBİ

EK 10

T.C.
KADIKÖY KAYMAKAMLIĞI
İlçe Emniyet Müdürlüğü

Sayı : B.05.1.EGM.4.34.58858-(62217)-**2012/**..... .../01/2013

Konu : Harddisk Talebi

..... CUMHURİYET BAŞSAVCILIĞINA
(Soruşturma No: 2012/70344)

İlgi : ..... C. Başsavcılığının .../.../2012 tarihli ve 2012/xxxx sayılı yazısı.

İlgi sayılı yazı ile gereği için Şube Müdürlüğümüze gönderilen talimatta, müşteki ..... tarafından verilen şikayet dilekçesinde; .....bildirilerek gerekli soruşturmanın yapılması istenmektedir.

Bu talebe binaen; yapılan çalışmalar ve yazışmalar sonucunda alınan cevabi yazılar doğrultusunda şüpheli olarak tespit edilen .....isimli şahıs ile ilgili olarak Kadıköy 7. Sulh Ceza Mahkemesinin .../.../2013 tarihli ve 2013/.....D.İşnolu kararına istinaden şüpheli .....isimli şahsın belirtilen **"Kadıköy Mah Kadıköy Sok. No:1 D:15 Kadıköy/İSTANBUL"** sayılı adresinde CMK' nın 116-117 ve 127. Maddeleri uyarınca arama yapılmış ve 134. Maddesi uyarınca bilgisayar ve benzeri cihazlara el konmuştur.

El konulan bu malzemeler üzerinde Şube Müdürlüğümüzce yapılacak olan bilgisayar ve benzeri cihazların incelemesinde; şüpheli disklerinin imajı (kopyası) başka bir boş diske alınıp incelemeye hazır hale getirilebilmesi için **1 TB kapasiteli 1 adet** harddiske ihtiyaç duyulmaktadır.

Bilgilerinize arz ederim.

.....
İlçe Emniyet Müdürü
3. Sınıf Emniyet Müdürü

EK :
İlgi sayılı yazı (6 Sayfa)

İst. Emn. Müd., BSM Şube Müdürlüğü Vatan Cad. B Blok Zemin Kat FATİH Ayrıntılı bilgi için irtibat: İ. ÇETİN P.M.
Telefon: (0 212) 636 22 94 Faks: (0 212) 636 29 83
e-posta: bilisim@icin.gov.tr

İNCELEME RAPORU 1

DİJİTAL MATERYAL
İmaj Alma Tutanağı ve İnceleme Raporu

İSTANBUL EMNİYET MÜDÜRLÜĞÜ
BİLİŞİM SUÇLARI VE SİSTEMLERİ ŞUBE MÜDÜRLÜĞÜ

RAPOR YAZIM TARİHİ	11.11.2009	
İNCELEME TALEP EDEN BİRİM	Bilişim Suçları ve Sistemleri Şube Müdürlüğü	
EVRAK TARİHİ	27.10.2009	**Sayısı:** B.05.1.EGM.4.34.00.58.04-2009/2779
KARARI VEREN MAHKEME	Kadıköy 1.Sulh Ceza Mahkemesi	
KARAR TARİHİ	23.10.2009	**Değişik İş No:** 2009/1472
KONUNUN ÖZETİ	Kadıköy Cumhuriyet Başsavcılığının 23.10.2009 tarih ve 2009/57645 sayılı soruşturması kapsamında Bilişim Sisteminin İşleyişini Engelleme veya Bozma suçu ile ilgili olarak Bilge isimli şahıstan ele geçirilen 500 GB kapasiteli sabit diskin incelenmesi istenmektedir.	

İNCELENECEK MATERYALİN TEKNİK ÖZELLİKLERİ

TÜRÜ	Sabit disk
MARKA	Western Digital
S/N	WXN509S45476
KAPASİTESİ	500 GB

DÜŞÜNCELER:

Bilge isimli şahsa ait olan yukarıda teknik özellikleri yazılı Western Digital marka sabit diskin var olan veri bütünlüğünü bozacak hiçbir **silme, ekleme ve değiştirmeye** yönelik müdahale yapılmadan imajı (diskin fotoğrafı) alınmış, imaja ilişkin Hash bilgisi tespit edilmiştir. Alınan imaj üzerinden yapılan teknik inceleme neticesinde ise;

Materyalin Fotoğrafı

----------Start of Log entry----------
Created: 2009-10-27 14:18 yıl/ay/gün
Closed : 2009-10-27 16:41 yıl/ay/gün
----------Disk-to-File Results----------
# of sectors: 976,773,168 (500.1 GB)
Chunk size in sectors: 7,812,500 (4.0 GB)
MD5 : 6aafc0e211f2b760ffd5e665bc2bcac3
----------Source Disk----------
Model: WDC WD5000BEVT-22ZAT0
S/N: WD-WXN509S45476
Capacity in sectors reported Pwr-ON: 976,773,168 (500.1 GB)
----------Destination Disks----------
Model: MAXTOR STM31000333AS
S/N: 9TE1XMWW
Capacity in sectors reported Pwr-ON: 1,953,525,168 (1.0 TB)
----------End of Log entry----------

Hash: veri depolama ünitelerine kayıtlı bir bilginin kendisine özel dijital parmak izidir. Hash imzası dünyada bilgisayar kriminalistiğinde kullanılmakta olup bahse konu materyalin incelemesinde, materyal üzerindeki bir karakterin bile değişmesi durumunda Hash değişmektedir.

File Integrity: Delil Bütünlüğü anlamına gelmektedir. Karşılığında dijital medya üzerinde herhangi bir değişiklik yapılıp yapılmadığını gösteren ifade yer almaktadır.

Acquisition Hash: Dijital medya üzerinde incelemeye başlanmadan önce medyanın tamamının bit bit, imajı alınır ve inceleme imaj üzerinden yapılır. İmaj alınır iken lisanslı program tarafından MD5 algoritması ile oluşturulan imaj alma değerdir.

Verify Hash: Bu değer ise inceleme tamamlandıktan sonra incelenen dijital medya üzerinde herhangi bir değişiklik yapılıp yapılmadığının kontrol edilmesi amacıyla MD5 algoritması ile oluşturulan doğrulama değerdir. **Acquisition Hash** değeri ile **Verify Hash** değerlerinin birbirleri ile aynı olması bu incelenen dijital medya üzerinde hiçbir değişiklik yapılmadığı anlamına gelmektedir.

File Created: Dosyanın ilk olarak oluşturulduğu tarih anlamına gelmektedir.

Logical Size: Dosyanın mantıksal boyutu anlamına gelmektedir.

Full Path: Bir dosyanın dijital medya üzerinde tam olarak nerede (hangi klasörler altında) olduğunu gösterir.

Hash Value: Bir dosyanın MD5 algoritması ile oluşturulan değeridir.

Title: Belge Başlığı demektir. Raporda belirtilen Microsoft Office dosyalarına ait başlık bilgisi anlamına gelmektedir.

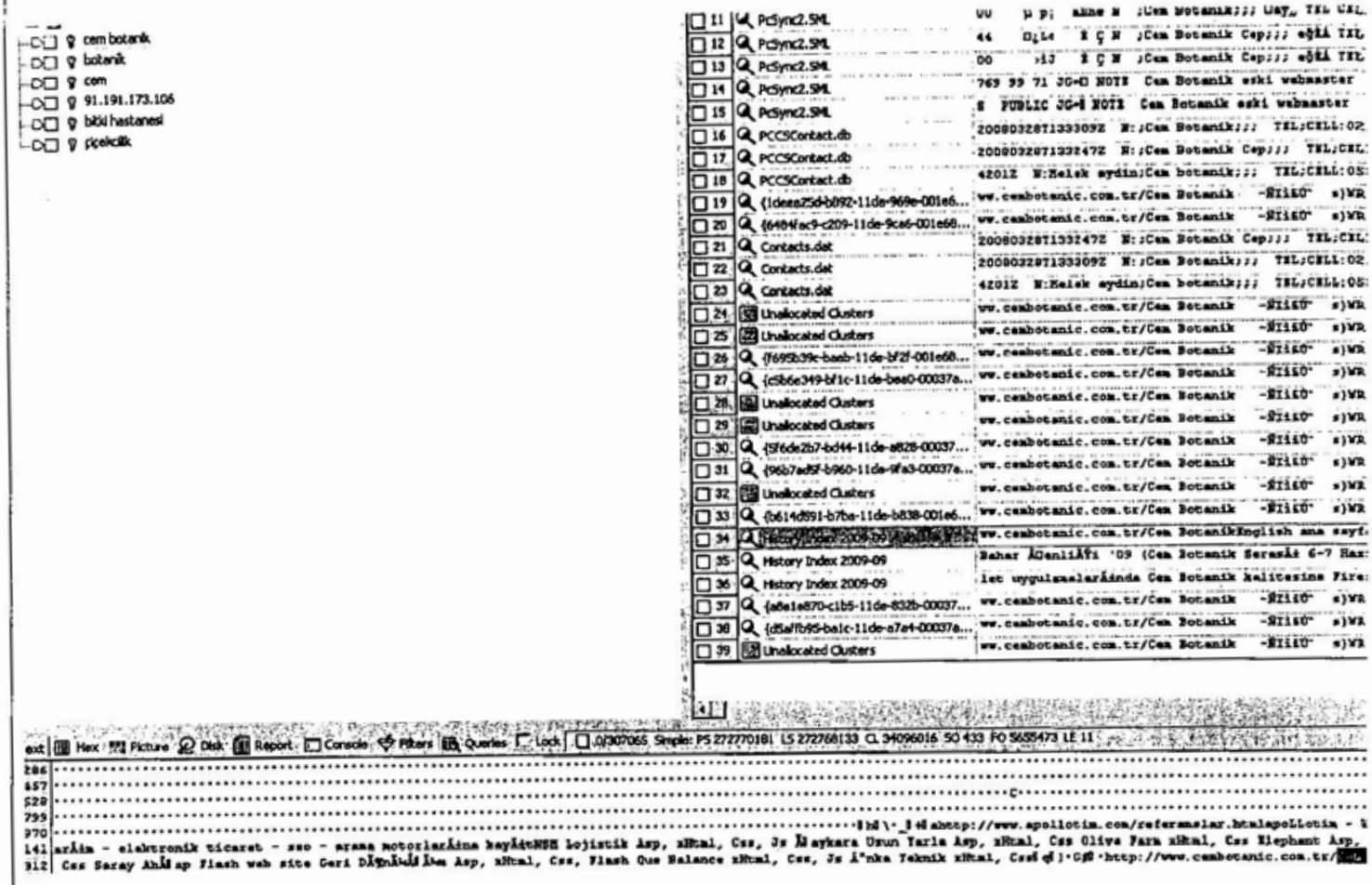
Subject: Belge konusu demektir. Raporda belirtilen Microsoft Office dosyalarının konusunu ifade etmektedir.

Author: Yazar demektir. Raporda belirtilen Microsoft Office dosyalarının hangi bilgisayar tarafından oluşturulduğu, yani oluşturulan bilgisayar adını ifade etmektedir.

Comments: Yorumlar demektir. Raporda belirtilen Microsoft Office dosyaları ile ilgili yapılmış olan açıklamaları ifade etmektedir.

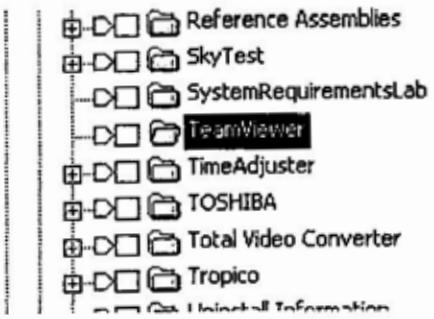
Sabit diskin mevcut klasörlerinde ve silinmiş dosyalarında "**doc, txt, xls, xml, pst, dbx, mdb, pdf, cdr, fh, rt ppt-pps,zip,rar ve htm**" uzantılı belgeler ile resim, (**jpg, jpeg, tiff, gif, bmp vb.**), video (**avi, wma, wmv, mp; mpeg, mov, awm vb.**) ve müzik dosyalarında inceleme yapılmıştır.

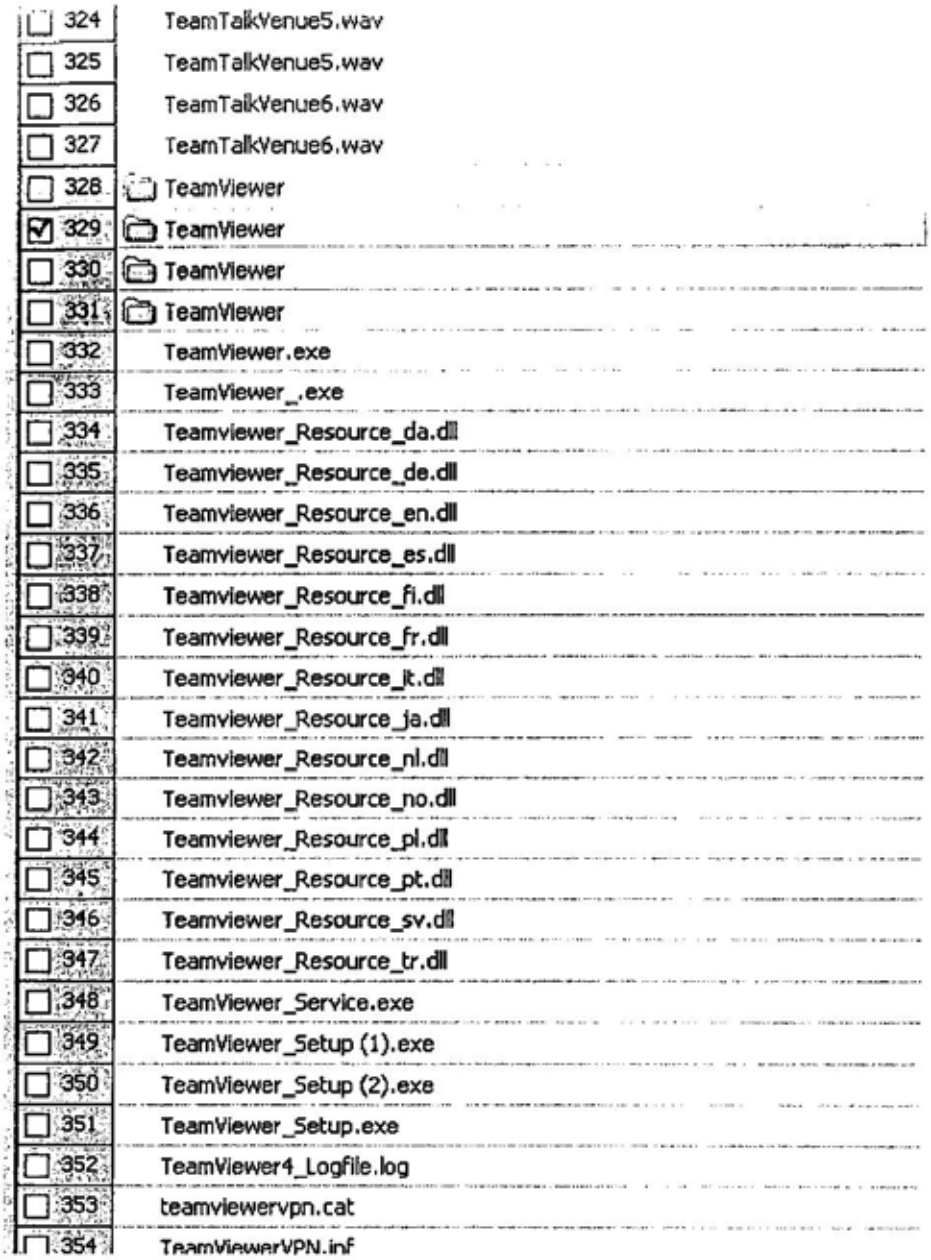
2- Sabit disk içerisinde www.c c.com.tr isimli internet sitesine erişim yapıldığı tespit edilmiştir.



3- Sabit disk içerisinde yapılan IP numarası aramasında müşteki şirketin bilgisayarlarına erişim sağlayan ve bilgileri silen IP numarası olarak bilinen 91.191.173.106 isimli IP numarasına rastlanmamıştır. Tarafımızdan yapılan IP aramasına ilişkin txt uzantılı belge imaj diski içerisine kopyalanmıştır.

4- Sabit disk içerisinde team viewer isimli uzak masaüstü programına rastlanmıştır.





SONUÇ OLARAK: Bahse konu sabit disk içerisinde yapılan teknik incelemede tarafımızdan yapılan tespitler yukarıda belirtilmiştir. Sabit diskin imajı 9TE1XMWW seri numaralı 1000 GB kapasiteli Maxtor marka sabit diske imaj diski ve imajlar tam, sağlam, çalışır vaziyette muhafaza altına alınmak üzere "Bilge_ _ _WesternDigital_WXN509S45476_500GB" klasörü adı altına kopyalanmıştır.

- Sabit disk içerisinde ve silinen alanında müşteki şirketin (**www. .com.tr**) internet sitesine erişim sağlandığına dair tespitler yapılmıştır.
- Sabit disk içerisinde müşteki şirketin bilgisayarlarına erişim sağlayan ve bilgileri silen IP numarası olarak bilinen 91.191.173.106 isimli IP numarasına rastlanmamıştır. Sabit disk içerisinde kullanılan IP numaraları **ip.txt** isimli belge içerisinde imaj diskine kopyalanmıştır.
- Özetle incelenen sabit disk içerisinde soruşturma evrakında geçen 91.191.173.106 isimli IP numarasına rastlanmamıştır.

243093
Adli Bilişim Büro Amiri
Başkomiser

274656
Adli Bilişim Büro Memuru
Polis Memuru

291285
Adli Bilişim Büro Memuru
Polis Memuru

280

İNCELEME RAPORU 2

RAPOR

(Teknik Analiz ve Hard Disk İnceleme Raporu)

Beyoğlu Cumhuriyet Başsavcılığının 02.08.2007 tarihli yazısı ve **2007/17464** sayılı soruşturması kapsamında;

Kartal 2.Sulh Ceza Mahkemesinin 15.08.2007 tarih ve 2007/1860 D. İŞ sayılı Bilgisayar Kayıtlarının İncelemesine İzin Verilmesi Kararı üzerine, **müşteki** **Tic AŞ'**ye ait www. .com isimli internet sitesine **12.07.2007** tarihinden beri aralıklarla **"DDOS Attack"** denilen ve hedef bilişim sisteminin bandwith kaynaklarını tüketerek internet ortamına servis vermesini imkânsız hale getiren ve sistemin devre dışı kalmasını sağlayan saldırıların yapılması olayı ile alakalı olarak yapılan çalışmalar neticesinde tespit edilen r **Sok. No: D: K: Maltepe-İSTANBUL** adresinden şüpheli **Batuhan** 'e ait aşağıda **özellikleri yazılı hard diskler** incelenmesi ve olayın aydınlatılabilmesi amacıyla **teknik inceleme için** Asayiş Şube Müdürlüğümüz Ar-Ge ve Bilgi İşlem Büro Amirliği **İnternet ve Bilişim Suçları Kısmı**mıza getirilmiştir.

DDOS Attack Nedir?

Açılımı ***"Distubuted Denial of Service"***dir ve Türkçe olarak dağıtılmış Servis Sömürüsü anlamına gelir. Bu saldırının yapılış şekli şöyledir. Bir saldırganın daha önceden tasarladığı veya hack yolu ile hazırladığı **birçok** makine (3. Şahıslara ait bilgisayarlara yüklenmiş trojanlar) üzerinden hedef sisteme (*bilgisayara veya hosta*) saldırı yaparak hedef sistemin kimseye hizmet veremez hale gelmesini, sistemin trafiğini arttırarak işlemez hale gelmesini amaçlayan bir saldırı çeşididir. Kısaca bu saldırı şekli sistemi engellemek, bozmak ve işlemez hale getirmek için bilgisayar korsanları tarafından kullanılır. Koordineli olarak yapılan bu işlem hem saldırının boyutunu artırır hem de saldırıyı yapan kişinin gizlenmesini sağlar. Bu işlemleri yapan araçlara **Zombi Bilgisayar** denir. Bu saldırı çeşidinde saldırganı bulmak zorlaşır. Çünkü saldırının merkezinde bulunan saldırgan aslında saldırıya katılmaz. Sadece daha önceden etkisi altına aldığı bilgisayarları kullanarak yönlendirme yoluyla saldırı yapar. Eğer saldırı bir tek ip adresinden yapılırsa bir Firewall (bir çeşit bilişim güvenlik katmanı) bunu rahatlıkla engelliyebilir. Fakat saldırı daha yüksek sayıdaki ip adresinden gelmesi Firewall un devre dışı kalmasını sağlar (Log taşması firewall servislerini durdurur). İşte bu özelliği onu diğer **DoS** saldırısından ayıran en önemli özelliğidir.

İnceleme Yapılacak Bilgisayar ve Eklentileri Özellikleri:

1. **Western-Digital Marka WD1600 model WCANM2161062 seri numaralı 160 GB'**lık hard disk.
2. **Samsung Marka SP0802N model S00JJ60Y104312 seri numaralı 80 GB'**lık hard disk.
3. **Western-Digital Marka WD200 model WMAAV1766500 seri numaralı 20 GB'**lık hard disk.
4. **Western-Digital Marka WD2500JS model WCANKF242910 seri numaralı 250 GB'**lık hard disk

İncelemelerde Dikkate Alınacak Hususlar:

1- Bu hard disklerde **"DDOS Attack"** denilen ve hedef bilişim sisteminin bandwith (sitelerin maksimum hizmet trafiği genişliği) kaynaklarını tüketerek internet ortamına servis vermesini imkânsız hale getiren ve sistemin devre dışı kalmasını sağlayan saldırıların yapılması olayı ile alakalı bilgisayar dosyaları araştırılacak,

2- İncelenen hard disklerde **müşteki** [redacted] Tic AŞ'ye ait www. [redacted].com isimli internet sitesine **12.07.2007** tarihinden beri aralıklarla **"DDOS Attack"** denilen ve hedef bilişim sisteminin bandwith kaynaklarını tüketerek internet ortamına servis vermesini imkânsız hale getiren ve sistemin devre dışı kalmasını sağlayan saldırıların yapılması olayı ile alakalı yazışma veya Msn Messenger görüşmeleri araştırılacak,
3- Soruşturma kapsamında değerlendirilecek diğer bilgisayar dosyaları araştırılacak,
4- Yukarıda belirtilen hususlarla ilgili bilgisayar dosyaları tespiti durumunda delil olabilmesi amacıyla metin haline getirilecektir.

BİLGİSAYAR ve EKLENTİLERİNİN İNCELEMESİ

İncelenen bilgisayara ait hard diskin bir adet image kopyası alınacak ve kopya hard disk üzerinde inceleme işlemi yapılacak, inceleme neticesinde raporlama işleminden sonra image kopyası alınan hard diskin kopyalarındaki veriler dijital ortamda silinmek suretiyle imha edilecektir.

HARD DİSK İNCELEMESİ:

1-A) Hard Disk Özelliği:

- **Western-Digital Marka WD1600 model WCANM2161062 seri numaralı 160 GB.**

1-B) Hard Disk İncelemesi

Western-Digital Marka WD1600 model WCANM2161062 seri numaralı 160 GB'lık hard diskin bir adet kopyası alınmış ve kopyalama işleminden sonra asıl Hard Diske Hiçbir işlem yapılmadan kopya üzerinde gerekli teknik incelemeye geçilmiştir.

1-C) Hard Disk İnceleme Neticesi:

Western-Digital Marka WD1600 model WCANM2161062 seri numaralı 160 GB'lık hard diskin kopyası üzerinde, yukarıda belirtilen konularla alakalı olarak, kullanıcısı veya kurulu işletim sistemi tarafından **silinmiş ve/veya silinmemiş** bilgisayar dosyaları üzerinde yapılan incelemede;

- Yapılan ilk incelemede bilgisayarın incelenen hard diskinin (*bilgisayar zaman birimi itibariyle*) **22.04.2007 günü saat 07.56 sıralarında kullanıcısı tarafından formatlanarak**, önceki tüm verilerin silinerek yeniden Microsoft Inc. İsimli firmaya ait **Windows XP tr** işletim sisteminin kurulduğu anlaşılmıştır.

- Hard disk içeriğinde yapılan incelemede bu hard diskin takılı olduğu bilgisayar dâhilinde [redacted].com isimli E-posta adresi kullanılarak diğer 3.şahıslara ait e-posta adresleri ile Msn Messenger yazışmaları yapıldığı ve bu yazışmaların kullanıcı tarafından kaydedildiği görülmüştür. Bu yazışmalar incelendiğinde 09.08.2007 tarihinde saat **21.34** ile **21.46** arasında thel [redacted]l@hotmail.com isimli e-posta adresi ile yazışma yaptığı ve yazışma sırasında müşteki [redacted] **'e Tic AŞ'**ye ait www. [redacted].com isimli internet sitesine yapılan DDOS Attacklar ile ilgili konuşmaların olduğu ve hatta şüpheli **Batuhan** [redacted] **'in** thebes [redacted]l@hotmail.com isimli e-posta kullanıcısından www. [redacted].com isimli internet sitesine saldırı yapılmasını istediği görülmektedir. Yapılan incelemede Msn Messenger konuşma sırasında ve sonrasında müştekinin www. [redacted].com isimli internet sitesine saldırı yapıldığı müştekinin incelenen bilişim sistemi bağlantı kayıtlarından anlaşılmış ve şüpheli **Batuhan** [redacted] **'in** müşteki [redacted] **Tic AŞ'**ye ait www.siberalem.com isimli internet sitesinin bilişim sistemine yapılan saldırıdan sorumlu olduğu **TESPİT EDİLMİŞTİR.** Tespiti yapılan [redacted]@f[redacted]ey.com isimli E-posta adresi ile thel [redacted]l@hotmail.com isimli e-posta adresi arasındaki konuşma metni raporumuzun ekinde **Ek–1** ve **Ek–2** içeriğinde bulunmaktadır.

- Yukarıda tespiti yapılan bilgisayar dosyasının 13.08.2007 günü saat 12.27 sıralarında bu hard diskin takılı olduğu bilgisayar dâhilinde kullanıcı marifetiyle silindiği de ayrıca **TESPİT EDİLMİŞTİR.**

- Bu bilgisayarda bulunan kayıtlı e-postalar üzerinde soruşturma kapsamında yapılan araştırma neticesinde; 13 Temmuz 2007 Cuma günü saat 13:41 sıralarında bu bilgisayara ozlem@ ı.com.tr isimli ve Özlem isimli bir e-posta kullanıcısından Şüpheli **Batuhan** 'e ait ı ı@d ost.com isimli e-posta adresine gönderilen elektronik posta içeriğinde, **müşteki** ile : isimli firma arasındaki soruşturmaya konu yazışma içeriklerinin şüpheli **Batuhan** 'e gönderildiği görülmüş ve şüpheli **Batuhan** , ile müştekinin önceki servis sağlayıcısı olan isimli firma ile fiziki bir bağlantısı olduğu anlaşılmıştır. Tespiti yapılan elektronik postaya ait içerik raporumuzun ekinde **Ek–3, Ek–4, Ek–5** ve **Ek–6** içeriğinde bulunmaktadır.

2-A) Hard Disk Özelliği:

- **Samsung Marka SP0802N model S00JJ60Y104312 seri numaralı 80 GB.**

2-B) Hard Disk İncelemesi

Samsung Marka SP0802N model S00JJ60Y104312 seri numaralı 80 GB'lık hard diskin bir adet kopyası alınmış ve kopyalama işleminden sonra asıl Hard Diske Hiçbir işlem yapılmadan kopya üzerinde gerekli teknik incelemeye geçilmiştir.

2-C) Hard Disk İnceleme Neticesi:

Samsung Marka SP0802N model S00JJ60Y104312 seri numaralı 80 GB'lık hard diskin kopyası üzerinde, yukarıda belirtilen konularla alakalı olarak, kullanıcısı veya kurulu işletim sistemi tarafından **silinmiş ve/veya silinmemiş** bilgisayar dosyaları üzerinde yapılan incelemede;

- Hard disk içeriğinde yapılan incelemede bu hard diskin takılı olduğu bilgisayar dâhilinde birçok değişik isimli E-posta adresi kullanılarak diğer 3.şahıslara ait e-posta adresleri ile Msn Messenger yazışmaları yapıldığı ve bu yazışmaların kullanıcılar veya kullanıcı tarafından kaydedildiği görülmüştür. Bu yazışmalar incelendiğinde çeşitli zaman birimlerinde ş s@ .ro isimli e-posta adresi ile 3.şahıslar arasında yazışma yapıldığı ve yazışmalar sırasında müşteki : **Tic AŞ**'ye ait www. .com ısimli internet sitesine yapılan DDOS Attacklar ile ilgili konuşmaların olduğu ve ayrıca başka sitelere de DDOS Attackların yapılması ile ilgili yazışmaların olduğu görülmüştür. Tespiti yapılan e-posta adresleri arasındaki konuşma metinleri raporumuzun ekinde **Ek–7** ve **Ek–8** içeriğinde bulunmaktadır.

3-A) Hard Disk Özelliği:

- **Western-Digital Marka WD200 model WMAAV1766500 seri numaralı 20 GB.**

3-B) Hard Disk İncelemesi

Western-Digital Marka WD200 model WMAAV1766500 seri numaralı 20 GB'lık hard diskin bir adet kopyası alınmaya çalışılmış ancak arızalı olduğundan dolayı bu hard disk üzerinde herhangi bir teknik inceleme yapılamamıştır.

4-A) Hard Disk Özelliği:

- **Western-Digital Marka WD2500JS model WCANKF242910 seri numaralı 250 GB.**

4-B) Hard Disk İncelemesi

Western-Digital Marka WD2500JS model WCANKF242910 seri numaralı 250 GB'lık hard diskin bir adet kopyası alınmış ve kopyalama işleminden sonra asıl Hard Diske Hiçbir işlem yapılmadan kopya üzerinde gerekli teknik incelemeye geçilmiştir.

4-C) Hard Disk İnceleme Neticesi:

Western-Digital Marka WD2500JS model WCANKF242910 seri numaralı 250 GB'lık hard diskin kopyası üzerinde, yukarıda belirtilen konularla alakalı olarak, kullanıcısı veya kurulu işletim sistemi tarafından **silinmiş ve/veya silinmemiş** bilgisayar dosyaları üzerinde yapılan incelemede;

- Bu hard disk içeriğinde soruşturma kapsamında değerlendirilebilecek herhangi bir bilgisayar dosyası tespit edilememiştir.

Netice Olarak;

Beyoğlu Cumhuriyet Başsavcılığının 02.08.2007 tarihli yazısı ve **2007/17464** sayılı soruşturması kapsamında; **Kartal 2.Sulh Ceza Mahkemesinin 15.08.2007 tarih ve 2007/1860 D. İŞ sayılı Bilgisayar Kayıtlarının İncelemesine İzin Verilmesi Kararı** üzerine, **müşteki** **Tic AŞ'ye** ait www. .com isimli internet sitesine **12.07.2007** tarihinden beri aralıklarla **"DDOS Attack"** denilen ve hedef bilişim sisteminin bandwith kaynaklarını tüketerek internet ortamına servis vermesini imkânsız hale getiren ve sistemin devre dışı kalmasını sağlayan saldırıların yapılması olayı ile alakalı olarak yapılan çalışmalar neticesinde tespit edilen **c. No: D: K: Maltepe-İSTANBUL** adresinden şüpheli **Batuhan** 'e ait yukarıda **özellikleri yazılı hard diskler** incelenmiş olup inceleme neticesinde ayrıntılı olarak yukarıda detaylar belirtilmiştir.

Özet olarak şüpheli **Batuhan** 'e ait toplam 4 (dört) adet hard diskten;

- 2 (iki) adet Hard disk içeriğinde soruşturma kapsamında değerlendirilebilecek bilgisayar dosyaları tespit edilmiş,
- Tespit edilen bu bilgisayar dosyalarından şüpheli **Batuhan** **müşteki** **Tic AŞ'ye** ait www. .com isimli internet sitesine yapılan saldırı ile ilgili olarak sorumlu olduğu,
- Sanal ortamda (internet ortamında) müştekinin bilişim sistemine yapılan saldırıyı organize ettiği ve gerçek saldırıyı th l@hotmail.com isimli e-posta adresi kullanıcısına yaptırdığı,
- Şüpheli **Batuhan** ile müştekinin önceki servis sağlayıcısı olan isimli firma ile fiziki bir bağlantısı olduğu,
- Şüphelinin zaman zaman 3. şahıslara ait başka sitelere de benzer saldırılar ile ilgili yazışmalar yaptığı **TESPİT EDİLMİŞTİR.**

İnceleme sonucu hazırlanan rapor üzerine, inceleme amacıyla kopyası oluşturulmuş kopya hard disk dijital ortamda silinmek suretiyle imha edilmiştir.

İşbu rapor 4 (dört) sayfa rapor ve 8 (sekiz) sayfa rapor eki olarak tarafımızdan tanzim edilerek altı birlikte imzalanmıştır. 15.08.2007 saat 20.00.

Dinçer AY
Başkomiser
İnt. ve Bilişim Suç. Kıs. Amr

Savaş YÖNDEM
Polis Memuru
İnt. ve Bilişim Suç. Mem.

FEZLEKE

T.C.
İSTANBUL VALİLİĞİ
Emniyet Müdürlüğü

K-Q TSE-ISO-EN 9000

Sayı : B.05.1.EGM.4.34.00.11.02.2007/(07-Ds.CBS:476)31010-2083 21/08/2007
Konu : Fezleke

BEYOĞLU CUMHURİYET BAŞSAVCILIĞINA

SORUŞTURMA NO	:	2007/17464
SUÇUN NOSU	:	07-Ds.CBS:476
SUÇUN NEVİ	:	Bilişim Sistemine Zarar Vermek, İşleyişini Engellemek
SUÇUN YERİ	:	Mh. Sk. No: Daire: Kat: **Maltepe - İSTANBUL**
SUÇUN TARİHİ	:	2007 Yılı Muhtelif Tarihler
SUÇUN DELİLİ	:	Teknik İnceleme Raporu, Telefon Tespiti
MÜŞTEKİ	:	**Reklamcılık ve Tic. A.Ş.**
VEKİLİ	:	Av.Doğan KARAKUŞ
ADRESİ	:	Tomtom Mh. İstiklal Cd. Mısır Apt. No:311 kat:6 D:23-24 Beyoğlu
ŞÜPHELİ – 1--	:	
AÇIK KİMLİĞİ	:	oğlu, 14.06.1981 - Kadıköy doğumlu, İstanbul –Üsküdar- nüfusuna kayıtlı, **TC:**
ADRESİ ve TEL.	:	Mh. Sk. No: Daire: Kat: **Maltepe – İSTANBUL** Ev: 0216
ŞÜPHELİ – 2--	:	**Özlem** – (Şahıs C.Savcılığında ifade verecekleri Avukatları vasıtasıyla bildirmişlerdir.)
ŞÜPHELİ – 3--	:	**Hakan** – (Şahıs C.Savcılığında ifade verecekleri Avukatları vasıtasıyla bildirmişlerdir.)
ŞÜPHELİ – 4--	:	**Güzin** – (Şahıs C.Savcılığında ifade verecekleri Avukatları vasıtasıyla bildirmişlerdir.)
ŞÜPHELİ – 5--	:	**Serdar** – (Şahıs C.Savcılığında ifade verecekleri Avukatları vasıtasıyla bildirmişlerdir.)
ŞÜPHELİ – 6--	:	**Ahmet** – (Şahıs C.Savcılığında ifade verecekleri Avukatları vasıtasıyla bildirmişlerdir.)
OLAYIN ÖZETİ	:	

İlgi

a) Beyoğlu C.Başsavcılığının 02.08.2007 tarih ve 2007/17464 soruşturma sayılı yazısı,
b) İstanbul Anadolu Yakası Türk Telekom Müdürlüğünün 14.08.2007 tarihli yazısı,
c) Kartal 2.Sulh Ceza Mahkemesinin 15.08.2007 tarih ve 2007/1860 sayılı kararı,
d) İstanbul Yakası Türk Telekom Müdürlüğü Bilişim Ağları Müdürlüğünün 13.08.2007 tarih ve 213557 sayılı yazısı,

Beyoğlu Cumhuriyet Başsavcılığının ilgi (a) sayılı yazısı ile yürütülen soruşturma gereği; müşteki Reklamcılık ve Tic. A.Ş.' vekili tarafından verilen şikayet dilekçesine istinaden şirkete ait www. .com isimli internet sitesine internet üzerinden DDOS atak denilen sanal saldırı yapmak suretiyle bilişim sisteminin işleyişini engelleyen, sistemi işlemez hale getiren ve sisteme kayıtlı üyelerin sisteme girişlerini engelleyen bilgisayar kullanıcılarının açık kimlik ve adres bilgilerinin tespit edilmesi istenmiştir.

DDOS atağı, bir bilişim sistemine sistemin kaldırabileceğinin çok üzerinde hizmet isteği gönderilmesi ve bu nedenle ana sistemin gelen bu hizmet isteklerine cevap verememesi olayıdır.

Soruşturma dosyası incelendiğinde, müşteki firmanın isimli bilgisayar firmasından aylık 27.000 YTL karşılığında hizmet aldığı ancak bu fiyatın fazla olmasını düşündükleri , hizmeti başka firmadan almak istedikleri ve bu nedenle Teklan isimli firmayla olan anlaşmalarını iptal ettirmek istedikleri anlaşılmaktadır.

./....

21.08.2007 tarih ve B.05.1.EGM.4.34.00.11.02.2007/(07-Ds.CBS:476)31010-2083 sayılı fezlekenin 2.sayfasıdır.

Şüphelilerden Özlem , ve Hakan arasındaki 31.07.2007 tarihinde saat 16.30 ve 17.09 saatleri arasındaki MSN görüşmelerinde;

Konuşan	İleti
Hakan	**Nereye ? Anlamadım?**
Özlem	**Siber**
Hakan	**Haa, inik , başladımı eğlence?**
Özlem	**he, bir saat oldu**
Hakan	**Eee, saat 16.41 ben bi bakim mi?**
Özlem	**Du bakim ne yapmış kankaya soriim**
Hakan	**Batu uyuyo mu he he ok indi mi**

Şeklinde sorduğu soruşturma dosyasından anlaşılmıştır. Batu isminden kasıt Batuhan olduğu şüpheliler arasındaki yazışmalardan dolayı değerlendirilmektedir. Bu konuşma esnasında da www. ı.com sitesinin bilişim sistemine zara verildiği ve işlemez hale getirildiği sistemi inceleyen görevliler tarafından tespit edilmiştir.

Şikayetçi firmanın şikayet dilekçelerinde belirtmiş oldukları Şüpheli Batuhan isimli ş. .s hakkında yapılan araştırmada şahsın 0216 numaralı sabit telefon hattını kullandığının belirlenmesi üzerine bu hattı kullanan abonenin açık kimlik ve adres bilgilerinin belirlenmesi için İstanbul Anadolu Yakası Türk Telekom Müdürlüğü ile gerekli yazışmalar yapılmış ve ilgi (b) sayılı cevap yazılarına kayden abone bilgisi aşağıdaki tablo şekliyle tespit edilmiştir.

S.N.	TELEFON NO	ABONE ADI	ADRES
1	0216	Aysel (Şüphelinin Annesi)	Sk. No: Daire: Kat: **Maltepe - İSTANBUL**

Yukarıda belirtilen Şüpheli Batuhan , isimli şahsın **"A. Mh. Sk. No: Daire: Kat: Maltepe - İSTANBUL"** sayılı adresinde 15.08.2007 tarihinde Kartal 2.Sulh Ceza Mahkemesinin ilgi (c) sayılı mahkeme kararına istinaden yapılan arama işlemi neticesinde;

- 1 adet Western Digital Marka WD1600 model WCANM2161062 seri numaralı hard disk,
- 1 adet Samsung Marka SP0802N model S00JJ60Y104312 seri numaralı hard disk,
- 1 adet Western Digital Marka WD200 model WMAAV1766500 seri numaralı hard disk,
- 1 adet Western Digital Marka WD2500JS model WCANKFA242910 seri numaralı hard diske el konulmuştur.

El koyulan ve özellikleri yukarıda belirtilen hard disklerin teknik olarak incelenmesi neticesinde ekte sunulan teknik inceleme raporlarından da anlaşılacağı üzere;

1. **1 (bir) adet Western-Digital Marka WD1600 model WCANM2161062 seri numaralı 160 GB harddisk içeriğinde bulunan;**

Hard disk içeriğinde yapılan incelemede bu hard diskin takılı olduğu bilgisayar dâhilinde destek@t urkey.com isimli E-posta adresi kullanılarak diğer 3.şahıslara ait e-posta adresleri ile Msn Messenger yazışmaları yapıldığı ve bu yazışmaların kullanıcı tarafından kaydedildiği görülmüştür. Bu yazışmalar incelendiğinde 09.08.2007 tarihinde saat **21.34** ile **21.46** arasında thebest @hotmail.com isimli e-posta adresi ile yazışma yaptığı ve yazışma sırasında müşteki **Reklâmcılık ve Tic AŞ**'ye ait www.s .com isimli internet sitesine yapılan DDOS Attacklar ile ilgili konuşmaların olduğu ve hatta şüpheli **Batuhan 'in** thebest l@hotmail.com isimli e-posta kullanıcısından www.: ı.com isimli internet sitesine saldırı yapılmasını istediği görülmektedir.

../....

Yapılan incelemede Msn Messenger konuşma sırasında ve sonrasında müştekinin www. .com isimli internet sitesine saldırı yapıldığı müştekinin incelenen bilişim sistemi bağlantı kayıtlarından anlaşılmış ve şüpheli **Batuhan** **'in** müşteki **Reklâmcılık ve Tic AŞ'**ye ait www. .com isimli internet sitesinin bilişim sistemine yapılan saldırıdan sorumlu olduğu **TESPİT EDİLMİŞTİR.**

Bu bilgisayarda bulunan kayıtlı e-postalar üzerinde soruşturma kapsamında yapılan araştırma neticesinde; 13 Temmuz 2007 Cuma günü saat 13:41 sıralarında bu bilgisayara ozlem@ .com.tr isimli ve Özlem isimli bir e-posta kullanıcısından Şüpheli **Batuhan** **'e** ait batuhan@ t.com isimli e-posta adresine gönderilen elektronik posta içeriğinde, **müşteki** ile isimli firma arasındaki soruşturmaya konu yazışma içeriklerinin şüpheli **Batuhan** **'e** gönderildiği görülmüş ve şüpheli **Batuhan** ile müştekinin önceki servis sağlayıcısı olan isimli firma ile fiziki bir bağlantısı olduğu anlaşılmıştır.

2. 1 (bir) adet Samsung Marka SP0802N model S00JJ60Y104312 seri numaralı 80 GB harddisk içerisinde bulunan;

Hard disk içeriğinde yapılan incelemede bu hard diskin takılı olduğu bilgisayar dâhilinde birçok değişik isimli E-posta adresi kullanılarak diğer 3.şahıslara ait e-posta adresleri ile Msn Messenger yazışmaları yapıldığı ve bu yazışmaların kullanıcılar veya kullanıcı tarafından kaydedildiği görülmüştür. Bu yazışmalar incelendiğinde çeşitli zaman birimlerinde ay @ .ro isimli e-posta adresi ile 3.sahıslar arasında yazışma yapıldığı ve yazışmalar sırasında müşteki **i Reklâmcılık ve Tic AŞ'**ye ait www. .com isimli internet sitesine yapılan DDOS Attacklar ile ilgili konuşmaların olduğu ve ayrıca başka sitelere de DDOS Attackların yapılması ile ilgili yazışmaların olduğu görülmüştür.

DDOS atak yapan bilgisayarların adreslerinin tespit edilmesi için müşteki firmanın sistemlerinden tespit etmiş oldukları ve şikayet dilekçelerinde belirtilen IP adresleri İstanbul Yakası Türk Telekom Müdürlüğü Bilişim Ağları Müdürlüğünden sorulduğunda ilgi (d) sayılı cevap yazılarına kayden tespit edilmiş, ancak tespit edilen adresler incelendiğinde adreslerin il dışında bulundukları ve muhtemelen şüpheli şahısların uzaktan erişerek bu bilgisayarları kullanıldıkları düşünülmektedir. Çünkü DDOS atak yapabilmek için birden fazla sayıda bilgisayara ihtiyaç duyulmakta ve bu bilgisayarlar genellikle olayı gerçekleştiren şahıs ya da şahıslarca virüs ve ya trojen bulaştırılarak elde edilen bilgisayarlardır.

İncelenmesi tamamlanan eşyalarda suç unsuru dosyaların tespit edilmesi üzerine; konu ile ilgili olarak 20.08.2007 tarihinde Beyoğlu Cumhuriyet Savcısı Sayın Hüseyin KAYNUN'a 0532 570 31 09 numaralı telefondan bilgi verilmiş, Sayın Savcı şüpheli şahsın gözaltına alınmasını ve mevcutlu olarak 21.08.2007 tarihinde Savcılıkta hazır edilmesi talimatını vermesi üzerine, Şüpheli Batuhan isimli şahıs göz altına alınmıştır.

Şüpheli **Batuhan** isimli şahsın müdafisi İstanbul Barosu 27778 sicil sayılı Avukatı Cihan ŞİMŞEK huzurunda ifadesi alınmış olup soruşturma dosyasına eklenmiştir.

Soruşturma dosyasından ve görevlilerimizin yapmış olduğu tespitlerden Hakan , Özlem , Batuhan ve thebesti @hotmail.com isimli e-posta kullanıcısı şahıs tarafından menfaat temin etmek amacıyla bilişim sistemine zara verdikleri ve sistemi erişilmez hale getirdikleri değerlendirilmektedir.

Şüpheli şahsın iletişimde bulunduğu ve www .com isimli internet sitesinin bilgilerini verdiği thebest l@hotmail.com isimli e-mail adresini kullanan şahsın açık kimlik ve adres bilgilerinin tespit edilebilmesi için e-mail adresinin kullanımı esnasındaki IP bilgilerinin tespit edilebilmesi için ilgili hizmet sağlayıcı firma olan Microsoft Corporation firması ile gerekli yazışmalar yapılmış, ilgili kurumdan cevap alındığında ayrıca Cumhuriyet Başsavcılığınıza bilgi verilecektir.

290

21.08.2007 tarih ve B.05.1.EGM.4.34.00.11.02.2007/(07-Ds.CBS:476)31010-2083 sayılı fezlekenin 4.sayfasıdır.

İncelenmesi tamamlanan ve içeriğinde suç unsuru dosyaların olduğu tespit edilen;

- 1 adet Western Digital Marka WD1600 model WCANM2161062 seri numaralı hard disk,
- 1 adet Samsung Marka SP0802N model S00JJ60Y104312 seri numaralı hard disk,
- 1 adet Western Digital Marka WD200 model WMAAV1766500 seri numaralı hard disk,
- 1 adet Western Digital Marka WD2500JS model WCANKFA242910 seri numaralı hard diski Adli Emanet Memurluğuna teslim edilmek üzere mühürlü olarak gönderilmiştir.

Soruşturma dosyasında adları geçen diğer şüpheli Özlem , Güzin , Serdar , Hakan ve Ahmet isimli şahısların şüpheli olarak ifadeleri için yapılan çalışmalarda şüphelilerin avukatı olduğunu söyleyen Av. Şenol ÇİLEK şüpheliler ile birlikte Beyoğlu Cumhuriyet Başsavcılığında bekledikleri ve C.Savcısına ifade vermek istediklerini bildirmişlerdir. Cumhuriyet Başsavcılığınızdan alınacak talimat doğrultusunda soruşturmaya devam edilecektir.

Olayla ilgili olarak yakalanan **Batuhan** isimli şahıs hakkında düzenlenen tahkikat evrakı ile birlikte mevcutlu olarak gönderilmiştir.

Tetkik ve kanuni gereğini arz ederim.

Mustafa KÖSE
Asayiş Şube Müdürü
3.Sınıf Emniyet Müdürü

EKİ :
Tahkikat Dosyası (... sayfa)

9

BİLİŞİM SUÇLARINA DAİR ÖRNEK VAKA ÇALIŞMALARI

1. Vaka
2. Vaka
3. Vaka
4. Vaka
5. Vaka

VAKA ANALİZİ 1

13.10.2013 tarihinde www.facebook.com alan adlı sitesindeki hesaba giriş yapıp vakit geçiren Ahmet Halis, hesap duvarında paylaşılan linkle ilgili yorumda "bu linkte şehitlerimize hakaret edilmektedir, protesto etmek için tıkla!" yazısını görüp linke tıklamıştır. Linke tıkladığı anda Facebook hesabından çıkış yaptığı zannıyla önüne gelen Facebook giriş sayfasına kullanıcı adı ve şifresini girerek siteye tekrardan girmiştir.

Bora Açıkgöz, Facebook gibi sosyal medya sitelerinin, bankaların vb. web sayfalarının bir kopyasını yapıp kullanıcının hesap bilgilerini çalmayı amaçlayan sahte yazılımlar üretmektedir. Bu yolla Ahmet Halis'in Facebook hesap bilgilerini ele geçiren Bora Açıkgöz, Ahmet Halis'in arkadaş listesindeki kişilerle Facebook Chat üzerinden iletişime geçerek kendisinin Ahmet Halis olduğuna inandırmıştır.

Ceren Has da Bora Açıkgöz'ün bu şekilde iletişime geçtiği kişilerden biridir. Bora Açıkgöz, Ceren Has'a "Maddi anlamda sıkıntıda olduğunu, belirtmiş olduğu IBAN numarasına 250 TL yatırırsa kendisine 10 gün sonra almış olduğu bu borcu ödeyeceğini" belirtmiştir. Bunun üzerine Ceren Has, Ahmet Halis 'in zor durumda olduğunu düşünerek belirtilmiş olan IBAN numarasına 250 TL yatırmıştır.

Ceren Has parayı yatırdıktan sonra, Ahmet Halis'i merak edip telefonla aramıştır. Ceren Has, bu telefon konuşmasında, kendisi ile Facebook'ta konuşan kişinin Ahmet Halis olmadığını, Ahmet Halis'in böyle bir borç talebinde bulunmadığını öğrenmiştir. Ahmet Halis ise Facebook hesabının ele geçirildiğini ve arkadaşlarıyla iletişime geçilip bu şekilde kendi adına borç para istendiğini öğrenmiştir.

Ahmet Halis ve Ceren Has bu olay üzerine karakola giderek suç duyurusunda bulunmuşlardır.

SORULAR

1. Olaydaki suç tiplerini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.

2. Bora Açıkgöz'ün suç işlerken kullanmış olduğu teknik yöntem hangisidir, açıklayınız.

3. Şüphelinin tespiti için hangi bilgilere neden ihtiyaç olduğu ve bu bilgilerin hangi makamlardan elde edileceğini tespit ediniz.

4. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.

5. 5651 sayılı Kanun'a göre Facebook'un hukukî statüsü nedir, açıklayınız.

6. Log kayıtlarının Facebook'tan temin edilmesi için hangi usulün izlenmesi gerektiğini açıklayınız.

7. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

CEVAPLAR

1. Olaydaki suç tiplerini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.

Ahmet Halis'e karşı Bilişim Sistemine Girme (TCK 243) suçu, Ceren Has'a karşı Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık suçu Bora Açıkgöz tarafından işlenmiştir.

2. Bora Açıkgöz'ün suç işlerken kullanmış olduğu teknik yöntem hangisidir, açıklayınız.

Bora Açıkgöz'ün Ahmet Halis'e karşı suç işlerken kullanmış olduğu teknik yöntem "phishing"tir. Phishing "Password" (Şifre) ve "Fishing" (Balık avlamak) sözcüklerinin birleştirilmesiyle oluşturulan, Türkçe'ye yemleme (oltalama) olarak çevrilmiş bir saldırı çeşididir. Phishing saldırıları son zamanların en gözde saldırı çeşidi olarak karşımıza çıkmaktadır. Yemleme yöntemi kullanılarak bilgisayar kullanıcıları her yıl milyarlarca dolar zarara uğratılmaktadır. Yemleme genelde bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmek amacıyla kullanılır. Bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahta sitelere yönlendirilir. Phishing saldırıları için 'Bankalar, Sosyal Paylaşım Siteleri, Mail Servisleri, Online Oyunlar vb. sahte web sayfaları hazırlanmaktır. Burada bilgisayar kullanıcısında özlük bilgileri, kart numarası, şifresi vb. istenir. E-posta ve sahte sitedeki talepleri dikkate alan kullanıcıların bilgileri çalınır.

Burada şunu da belirtmek gerekir, arama motorlarında bazı bankaların dolandırıcılar tarafından hazırlanan sahte web adreslerinin yer aldığı göz önüne alınırsa, bu saldırıların yaygın olduğu görülmektedir. Tedbir olarak banka adreslerinin, adres çubuğuna elle (manuel) olarak yazılması önerilebilir.

3. Şüphelinin tespiti için hangi bilgilere neden ihtiyaç olduğu ve bu bilgilerin hangi makamlardan elde edileceğini tespit ediniz.

a) Şüphelinin dolandırıcılık fiili gerçekleştirildiği iddia edilen bilgisayarın IP bilgisine ihtiyaç vardır.

Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleri ile iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, internet protokolu standartlarına göre verilen adresi ifade eder.

İnternete bağlanan her bilgisayara internet servis sağlayıcı tarafından bir IP adresi atanır ve internetteki diğer bilgisayarlar bu bilgisayara verilen bu IP adres ile ulaşırlar.

IP adresleri dinamik ve statik olarak iki bölüme ayrılır. Ancak genel olarak dinamik IP adresi kullanılır. Dinamik IP adresleri zamana ve oturuma göre değişir. Çünkü servis sağlayıcı o an için boş olan IP adresini kullanıcıya atar. Statik IP adresi ise, zamana ve oturuma göre değişmeyen adresi ifade eder. Ancak sistem yöneticisi tarafından tanımlanıp değiştirilebilir.

Ayrıca alan adları için de bir IP adresi vardır. Bir internet sayfasını yazdığımız

kısmına (ağ tarayıcı) bu IP adresi de yazılarak bağlanılabilir. Ancak bu rakamları yazmak pratik ve akılda kalıcı olmadığından alan adı IP adresine karşılık gelen bir alan adı sistemi kullanılmaktadır.

b) Şüphelinin dolandırıcılık fiili gerçekleştirmek için para talep ettiği iddia edilen hesap numarasının ait olduğu kişinin bilgilerine ihtiyaç vardır. Bu bilgiler Banka'dan talep edilir.

4. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.

Şüphelinin tespit edilmesinden sonra başkaca bir suretle delil elde edilmesinin mümkün olmaması nedeniyle, CMK madde 134'e göre Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına hâkim tarafından karar verilir. Delillerin sağlıklı biçimde toplanabilmesi, olay yerine yapılan ilk müdahalenin ne kadar sağlıklı olduğuna bağlıdır. Adlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde edilirken bilgisayardaki verilerin mevcut hâli ile yedeği alınmalı, bilgisayar iade edilmeli ve yapılacak arama işlemi bu yedek üzerinde yapılmalıdır. Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifre çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar gecikme olmaksızın iade edilir. Şüphelinin bilgisayarında bizzat bulundurulması suç olan kredi kartı şifreleri, çocuk pornografisi vb. mevcut ise yedeklerin verilmemesi gerekmektedir. Çıkartılacak yedekten şüpheliye veya vekiline örnek verilmesi bu kişilerin isteğine bırakılmıştır. Ancak şüpheliye örnek isteyip istemediği sorulup bu husus kayıt altına alınmalıdır. Delil toplamadaki başarı oranı, bilişim suçlarıyla mücadelenin önemli bir göstergesidir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz saptanması ve zarar görmeden toplanması, ilk olay yeri müdahalesinin düzgün yapılmasıyla mümkündür. Adli bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde etme çalışması sırasında, olay yerinde varsa (örneğin güvenliği sağlayan) konu hakkında bilgi ve tecrübesi olmayan kişilerin aygıt ve sisteme müdahaleleri kesinlikle engellenmelidir. Kriminal inceleme yürütülürken elektronik deliller de toplanmalı, bunun için öncelikle delillerin nerede ve hangi formatta olduğu, nasıl depolandığı tespit edilmelidir. Sonrasında, ortamda bulunan elektronik donanımların çalışma biçimleri ve birbirlerine bağlılıkları tespit edilerek buna göre hareket edilir. Örneğin, olay yerinde kapalı konumda bulunan bir bilgisayar varsa kesinlikle açılmamalı; açık bir bilgisayar ise kesinlikle doğrudan kapatılmamalıdır. Bilgisayarın açılması hâlinde işletim sistemi çalışacak ve bilgisayar verileri işlemeye başlayacaktır. Bunun sonucu ise, verilerin üzerine yeniden veri yazılması ve potansiyel delillerin kaybı olabilecektir. Bilgisayar açık ise kesinlikle hiçbir program çalıştırılmamalı, hatta bilgisayar kapatılmamalıdır. Herhangi bir programın çalışması, bir potansiyel delilin kaybı anlamına gelebilir. Bilgisayar çalışıyor konumda fakat ekranı siyah ise, ekranın açık olup olmadığı kontrol edilmeli, sonrasında fare (mouse) oynatılarak görüntünün gelmesi sağlanmalıdır. Çalışmakta olan bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesi, doğal olarak o anda ve olay yerinde mümkün olamayacaktır. Bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gereklidir. Kapatılması dahi veri kaybına yol açabilecek

bir donanımın götürülmesi durumunda öncelikle bilgisayar üzerinde bulunan ve çalışma konumundan çıkınca yok olabilecek tüm bulgular tespit edilerek belirlenmeli, kesinlikle ekran görüntüsü fotoğraflanmalı, çalışan programlar varsa not edilmeli ve bilgisayar kapatılmayarak arkadaki güç kablosu çekilmelidir. Bunun yapılması belki birtakım verilerin kaybına yol açabilecekse de, delillerin bütünlüğünün bozulmasının önüne geçecektir. Delillerin tümünün kaybındansa, az miktar verinin kaybı daha tercih edilir bir durumdur. Kaldı ki, bilgisayardaki tüm delillere adlî bilişim uzmanlarınca ve laboratuar ortamında çeşitli analizler yapılmaksızın ulaşılması çok olası bir durum değildir. Delil araştırma amaçlı olarak yapılacak incelemeler, donanımlar üzerinde değil, alınan kopyaları üzerinde yapılmalıdır. Bu, donanımlar içerisindeki verilerin kaybını önleyecektir. Aygıtlardaki verilerin sağlıklı kopyalarının alınması çok önemlidir. Adlî bilişimde yapılan birebir kopyalama işlemine imaj (birebir kopya) denilmektedir. Bu kopyalama, sistemdeki tüm verilerin, özel yazılımlar veya donanımlar kullanmak suretiyle ve bit-bit başka bir ortamda bir örneğinin (imajının / birebir kopyasının) oluşturulması suretiyle yapılır. Adlî imajın önemi, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşma olanağını vermesidir. Sistemden imajı alınmış verilerin tümünün gözle görünür hale getirilmesinden sonra analiz aşamasına geçilecektir. Adlî bilişimin son safhası raporlama ve yetkili makama sunma safhasıdır. Raporlama safhası, hukukî bir değerlendirmeyi içermektedir. Değerlendirmeyi adlî bilişim uzmanı değil, kolluk yapar. Adlî bilişim uzman(lar)ının inceleme aşamasından geçmiş verilerden hangilerinin delil olabileceği, o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilir ve adli makamlara sunulur.

5. 5651 sayılı Kanun'a göre Facebook'un hukuki statüsü nedir, açıklayınız.

5651 sayılı Kanun ile içerik sağlayıcıların, yer sağlayıcıların ve erişim sağlayıcıların tanımı yapılmış ve sorumluluk ve yükümlülükleri düzenlenmiştir. Facebook Amerika menşeli bir site olduğu için Türk Hukuku'na tabi olmasa da Türkiye'de ofisinin bulunması hâlinde 5651 sayılı Yasa'nın 2. maddesinin 1. fıkrasının m bendinde, "hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir." şeklinde tanımlandığı üzere yer sağlayıcı konumunda olacaktır. Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Yer sağlayıcı, yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, 5651 sayılı Kanunun 8'inci ve 9'uncu maddelerine göre haberdar edilmesi hâlinde ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür. 5651 sayılı Yasanın 8. maddesinin 10. fıkrasına göre, koruma tedbiri niteliğinde verilen erişime engelleme kararının varlığı hâlinde, ilgililerin hukuka uygun bir şekilde kendisine ilettiği erişim engelleme kararını teknik açıdan imkânı olduğu halde yerine getirmeyen yer sağlayıcıların sorumlularına, eylem daha ağır bir cezayı gerektirmediği takdirde altı aydan iki yıla kadar hapis cezası verilecektir. Trafik bilgisi internet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerlerin bütünüdür. Yer sağlayıcılar, trafik bilgilerini altı ay saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü tutulmuşlardır.

6. Log kayıtlarının Facebook'tan temin edilmesi için hangi usulün izlenmesi gerekir, açıklayınız.

Bilişim suçlarının en önemli özelliklerinden birini de bu suçların genellikle

sınır aşan bir biçimde işlenmesi ve buna bağlı olarak uluslararası bir boyutunun olmasıdır. Dolayısıyla günümüzde bilişim suçlarıyla ilgili olarak uluslararası kuruluşlar ve çalışmalar olduğu gibi, çok ciddi hukuksal düzenlemeler de bulunmaktadır. Nitekim ulusal hukuklarda konuyla ilgili olarak yapılan düzenlemelerin çoğu ya uluslararası düzenlemelerden alınmış ya da bunlara uyumlu hâle getirilmiştir. Özellikle Avrupa Siber Suç Sözleşmesinin yürürlüğe girmesinden sonra taraf ülkeler için durum tam bu şekildedir. Türkiye açısından uluslararası adlî yardımlaşmaya ilişkin çok taraflı ve iki taraflı anlaşmalar bulunmaktadır. Türkiye'nin Amerika Birleşik Devletler ile arasında ceza istinabe konusunda ikili antlaşmalar bulunmaktadır. Uluslararası istinabeye ilişkin sözleşmelerden biri de Avrupa Siber Suçlar Sözleşmesi'dir. Siber Suçlar Avrupa Sözleşmesi'ni; Amerika Birleşik Devletleri, İngiltere, Fransa, Almanya, Japonya'nın da dâhil olduğu 10 devlet imzalamış ve ulusal parlamentosunda onaylayarak yürürlüğe koymuştur. Türkiye'nin de arasında olduğu 37 ülke Sözleşmeyi imzalamış ancak henüz parlamentosundan geçirmemiştir. Sözleşme 2012 yılı Aralık ayında onay için TBMM'ye gönderilmiş, Meclis Dışişleri Komisyonunda kabul edilerek Genel Kurula sevk edilmiştir. Hâlen Genel Kurul gündemine alınması beklenmektedir.

Siber suçlarda şüpheliye ulaşmak için en yaygın şekilde kullanılan yöntem şuça konu işlem yapılırken kullanılan IP numarası tespit edilerek IP numarasının tahsis edildiği internet abonesini belirlemektir. Bu tür suçlarla ilgili olarak yapılan uluslararası adlî yardımlaşma taleplerinin büyük çoğunluğu da IP numarası veya trafik verisinin ilgili firmadan temin edilmesi talebini içermektedir. Facebook gibi yer sağlayıcı firmalar kural olarak adlî makamların kendilerinden talep ettikleri IP bilgisi, trafik verisi veya içeriğe ilişkin bilgileri vermemekte bunun adlî yardımlaşma yoluyla firma merkezinin bulunduğu devlet yapılacak bir taleple elde edilebileceğini belirtmektedirler. İstisna olarak Facebook'un belli şartlarda IP veya trafik bilgisini doğrudan vermesi gösterilebilir. Facebook; intihara teşebbüs, öldürmeye teşebbüs, kayıp bir şahsın bulunması veya çocukların cinsel istismarı suçlarını acil husus kabul ederek soruşturma makamlarımız tarafından doğrudan talepte bulunulduğunda IP veya trafik bilgilerini vermektedir. Ancak olayımızda bu şekilde bir suç işlenmediğinden adlî yardımlaşma prosedürü işletilerek log kayıtlarının talep edilmesi gerekmektedir.

7. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

a) Müşteki savcılık makamından havaleli dilekçe ile birlikte ilçe emniyet müdürlüğüne gelir.

b) Müştekinin dilekçedeki/savcılık ifadesindeki bilgiler yeterli değilse ayrıntılı ifadesi alınır.

c) Site ile ilgili internet üzerinden www.tib.gov.tr adresinden whois sorgusu yapılır.

d) Site hakkında web tespit raporu tanzim edilir.

e) Dolandırıcılık yapıldığı tarihlerdeki hacklenen hesaba giriş yapılan bilgisayarın IP numaraları, ABD ile Türkiye arasında 1981 tarihli Türkiye Cumhuriyeti İle Amerika Birleşik Devletleri Suçluların Geri Verilmesi Ve Ceza İşlerinde Karşılıklı Adli Yardım Antlaşması kapsamında adlî yardımlaşma yoluyla ABD'den istenmelidir. Zîra adlî makamlarımızın doğrudan kendilerin gerçekleştirmiş oldukları talepleri yerine getirmemektedirler. Ancak insan hayatının korunması için önemli olan intihara teşebbüs, öldürmeye teşebbüs, kayıp bir şahsın bulunması veya çocuk istismarı gibi suçları acil husus kabul ederek adli makamlarımız tarafından doğrudan başvurulduğunda trafik veya IP bilgilerini vermektedir.

f) Ceren Has'ın istenilen parayı Zakkum Bankası'na yatırmış olduğu hesap numarasının sahibine ait açık adres ve kimlik bilgileri ve bahse konu işlem bilgileri bankadan talep edilir.

g) IP bilgileri ülkemiz saatine çevrilir.

h) Çözümleme yapılan IP adresi ile ilgili whois sorgusu yapılır.

i) Şüpheli IP adresi servis sağlayıcıdan (Türk Telekom'dan) sorulur. Son 3 aylık uygulamada; TİB'in yetkilendirmiş olduğu Emniyet Müdürlüğü'nde bulunan birim sayesinde şüphelinin IP adresini tespit için servis sağlayıcılara yazı yazma gereksinimi sona ermiştir. Söz konusu birim, çok daha kısa bir süre içinde şüphelinin IP bilgilerini tespit edebilmektedir.

j) İlgili firma ve kuruluşlardan gönderilen kimlik ve adres bilgisi kontrol edilerek ve başkaca delillerin de aynı kişiyi göstermesi sonucunda şüpheli şahıs tespit edilir.

k) Savcılığın talimatı doğrultusunda başka suç ve suç delillerinin elde edilebilmesi amacıyla şüpheli şahsın ikametine veya işyerine arama, el koyma ayrıca arama sonucu elde edilecek olan bilgisayar ve diğer dijital materyaller üzerinde CMK'nın 134. Maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde, hard disklerinde arama, inceleme, izin talebinde bulunulur.

l) Arama esnasında tespit edilen dijital materyallerin imajlarının alınarak incelenmesinde kullanılmak üzere ilgili Cumhuriyet Savcılığı'ndan el konulan materyallerin %30 fazlası hard disk fazlası talebinde bulunulur.

m) Tespit edilen dijital materyaller üst yazı ile içeriğinde inceleme izni bulunan mahkeme kararı ve soruşturma evrakının bir örneği ile Siber Suçlarla Mücadele Şube Müdürlüğü'ne elden teslim edilir.

n) İnceleme sonucunda hazırlanan rapor ve dijital materyaller soruşturma birimince teslim alınır.

o) Rapor ve diğer deliller doğrultusunda suçla ilgili şüpheli şahsın konu hakkında ayrıntılı ifadesi alınır.

ZAKKUM BANK

Hesap Adı: Ceren Has **Hesap Şubesi: Zeytinburnu**

Hesap Tipi: Cari Hesap **Hesap Numarası: 1234 1234 1234**

Hesap Tarihi:20 Kasım 2013 **Sayfa:1**

Tarih	İşlem Türü	Açıklama	Ödenen	Bakiye
01.Ara.13		Açılış Bakiyesi		25.000,00 TL
02.Ara.13	ATM	Para çekimi	700,00 TL	24.300,00 TL
04.Ara.13	ATM	Para çekimi	500,00 TL	23.800,00 TL
05.Ara.13	EFT	TR 83 6758 5467 4360 IBAN numarasına Para gönderimi	50,00 TL	23.750,00 TL
08.Ara.13	Havale	TR 23 6758 5467 4380 IBAN numarasına Para gönderimi	150,00 TL	23.600,00 TL
10.Ara.13	ATM	Para çekimi	200,00 TL	23.400,00 TL
13.Ara.13	EFT	TR 34 6758 5467 4558 IBAN numarasına Para gönderimi	100,00 TL	23.300,00 TL
14.Ara.13	Havale	TR 43 6758 5467 6558 IBAN numarasına Para gönderimi	25,00 TL	23.275,00 TL
18.Ara.13	ATM	Para çekimi	100,00 TL	23.175,00 TL
20.Ara.13	ATM	Para çekimi	250,00 TL	22.925,00 TL
22.Ara.13	EFT	TR 64 6758 5467 4358 IBAN numarasına Para gönderimi	250,00 TL	22.675,00 TL
25.Ara.13	ATM	Para çekimi	500,00 TL	22.175,00 TL
26.Ara.13	Havale	TR 46 645 5465 4658 IBAN numarasına Para gönderimi	200,00 TL	21.975,00 TL
29.Ara.13	ATM	Para çekimi	300,00 TL	21.675,00 TL
31.Ara.13	EFT	TR 56 6758 5467 2358 IBAN numarasına Para gönderimi	150,00 TL	21.525,00 TL

VAKA ANALİZİ 2

Süleyman Başkol, kredi kartından para çekmek için Zakkum Bankası'na gitmiştir. ATM'de kart yuvasına kartını yerleştirmeye çalıştığı sırada kartı sıkışmıştır. Arka sırasında bekleyen Bihter Zil kendisine yardım teklifinde bulunmuş ve kartı kurtarmak için kartın şifresini öğrenip birtakım denemelerde bulunmuş; ancak başarılı olamamıştır. Bunun üzerine Süleyman Başkol, kartını kurtaramayacağını düşünerek olay yerinden ayrılmıştır. Akabinde, Bihter Zil kart yuvasına kurmuş olduğu düzenek sayesinde kartı çıkararak öğrenmiş olduğu şifreyle karttaki parayı çekmiştir.

Bihter Zil, Zakkum Bankası'nın ATM'sinden Süleyman Başkol'un kart şifresi, hesap numarası, diğer şifreleme unsurlarını ele geçirip bu bilgileri kendi adına basılmış plastik kartın manyetik şeridine söz konusu bilgileri kodlamaya yarayan encoder adlı bir araçla geçirerek sahte kredi kartı üretmiştir. Böylece görünüşte Bihter Zil'in hamil olduğu, ancak gerçekte Süleyman Başkol'a ait banka hesabıyla ilişkilendirilmiş sahte bir kredi kartı üretmiştir. Üretmiş olduğu bu banka kartıyla, internet üzerinden **www.abc.com**, **www.123.com** sitelerinden alışveriş yapmış, Amerika menşeli **www.xyz.com** adlı arkadaşlık sitesine belli bir ücretle 5 aylık üye olmuştur.

Selin Kaptı, Bihter Zil'in ücretsiz program indirme sitelerinden birine yüklediği kötü niyetli bir yazılımı, güvenli olduğunu düşünerek bilgisayarına indirmiştir. Bihter Zil, bu şekilde Selin Kaptı'nın bilgisayarına erişme imkânı elde ederek Selin Kaptı'nın bilgisayarında yaptığı her türlü işlemi, bilgisayar ekranını ve klavyesini takip etmiştir. Yaptığı takipler sonucunda Selin Kaptı'nın Zakkum Bankası'ndaki hesap bilgilerini ele geçirmiş ve hesaba girerek 100.000 TL'yi kendi hesabına havale etmiştir.

SORULAR

1. Bihter Zil'in Selin Kaptı'nın bilgisayarına erişmek için kullanmış olduğu teknik yöntem hangisidir, açıklayınız.

2. Olaydaki suç tiplerini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.

3. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.

4. 5651 sayılı Kanun'a göre www.abc.com, www.123.com ve www.xyz.com sitelerinin hukukî statüsü nedir, açıklayınız.

5. Log kayıtlarının www.xyz.com adlı arkadaşlık sitesinden temin edilmesi için hangi usulün izlenmesi gerektiğini açıklayınız.

6. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

CEVAPLAR

1. Bihter Zil'in Selin Kaptı'nın bilgisayarına erişmek için kullanmış olduğu teknik yöntem hangisidir, açıklayınız.

Bihter Zil'in Selin Kaptı'nın bilgisayarına erişmek için kullanmış olduğu teknik yöntem "Truva atıdır (trojan). Truva atı; yararlı gibi görünen ancak aslında zarara yol açan bilgisayar programlarıdır. Truva atları, insanların, meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya yöneltilmeleri yoluyla yayılır. Truva atları, ücretsiz

olarak yüklediğiniz yazılımlarda da bulunabilir. Güvenmediğiniz bir kaynaktan asla yazılım yüklemeyin.

Trojan "kurban"ının tahmin etmediği bir şekilde ve isteği olmaksızın, gizli ve genellikle kötü amaçlı bir faaliyette bulunan bir programdır. Virüsten farkı kendi kendini çoğaltmamasıdır (her ne kadar bu ayrım evrensel olarak kabul görmemişse de).

2. Olaydaki suç tiplerini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.

a) Bihter Zil'in Süleyman Başkol'a karşı işlemiş olduğu suç Başkasına Ait Banka Kartının Ele Geçirilmesi veya Elde Bulundurulması suçunu (TCK 245/1-1) işlemiştir.

b) Bihter Zil'in Bay Süleyman Başkol'un kartını kullanarak kendisinin hamil olduğu sahte banka kartı üretmesi Başkasına Ait Banka Hesaplarıyla İlişkilendirilerek Sahte Bank Kartı Üretimi Suçu (TCK 245/2) işlemiştir.

Bihter Zil sahte olarak üretmiş olduğu bu banka kartıyla **www.abc.com**, **www.123.com** sitelerinden alışveriş yaparak **www.xyz.com** adlı arkadaşlık sitesine belli bir ücretle 5 aylık üye olarak "sahte oluşturulan veya üzerinde sahtecilik yapılan bir bank kartını kullanmak suretiyle kendisine veya başkasına yarar sağlama suçunu" (TCK 245/3) işlemiştir.

Burada aynı maddenin iki fıkrasında düzenlenen iki ayrı suç tipinin birlikte işlenmesi konusunun tartışılması gereklidir. Failin sahte olarak üretilmiş ya da sahteleştirilmiş bir banka veya kredi kartını kullanarak kendisi veya başkası yararına haksız yarar elde edebilmesi için öncesinde bu kartı ya üretmesi ya satın alması ya da bir şekilde kabul etmesi gerekir. Bunlar dışında kartın elde edilmesi için kalan tek seçenek kartın bulunmasıdır. Ki fail bulduğu kartın sahte olduğunu bilemeyeceği için bu kez de kast unsuru gerçekleşmeyeceği için 3. Fıkrada yer alan suç oluşmayacaktır. Dolayısıyla 3. Fıkrada yer alan suçun işlenebilmesi için failin öncesinde ikinci fıkrada yer alan hareketlerden birisini gerçekleştirmesi gerekecektir. Buna göre ikinci fıkrada yer alan hareketler 3. Fıkradaki suç açısından cezalandırılmayan önceki hareketler olacaktır. Ancak Yargıtay failin hem kartı üretmesi ve hem de kullanması hâlinde her iki suçtan ayrı ayrı cezalandırılması gerektiği yönünde kararlar vermektedir.

c) Bihter Zil, Selin Kaptı'ya karşı "nitelikli hırsızlık suçunu" işlemiştir. (hırsızlık suçunu bilişim sistemlerinin kullanılması suretiyle işlenmesi)

3. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.

Şüphelinin tespit edilmesinden sonra başkaca bir suretle delil elde edilmesinin mümkün olmaması nedeniyle, CMK madde 134'e göre Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına hâkim tarafından karar verilir. Delillerin sağlıklı biçimde toplanabilmesi, olay yerine yapılan ilk müdahalenin ne kadar sağlıklı olduğuna bağlıdırAdlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye

indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde edilirken bilgisayardaki verilerin mevcut hali ile yedeği alınmalı, bilgisayar iade edilmeli ve yapılacak arama işlemi bu yedek üzerinde yapılmalıdır. Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifre çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar gecikme olmaksızın iade edilir. Şüphelinin bilgisayarında bizzat bulundurulması suç olan kredi kartı şifreleri, çocuk pornografisi vb. mevcut ise yedeklerin verilmemesi gerekmektedir. Çıkartılacak yedekten şüpheliye veya vekiline örnek verilmesi bu kişilerin isteğine bırakılmıştır. Ancak şüpheliye örnek isteyip istemediği sorulup bu husus kayıt altına alınmalıdır. Delil toplamadaki başarı oranı, bilişim suçlarıyla mücadelenin önemli bir göstergesidir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz saptanması ve zarar görmeden toplanması, ilk olay yeri müdahalesinin düzgün yapılmasıyla mümkündür. Adlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde etme çalışması sırasında, olay yerinde varsa (örneğin güvenliği sağlayan) konu hakkında bilgi ve tecrübesi olmayan kişilerin aygıt ve sisteme müdahaleleri kesinlikle engellenmelidir. Kriminal inceleme yürütülürken elektronik deliller de toplanmalı, bunun için öncelikle delillerin nerede ve hangi formatta olduğu, nasıl depolandığı tespit edilmelidir. Sonrasında, ortamda bulunan elektronik donanımların çalışma biçimleri ve birbirlerine bağlılıkları tespit edilerek buna göre hareket edilir. Örneğin, olay yerinde kapalı konumda bulunan bir bilgisayar varsa kesinlikle açılmamalı; açık bir bilgisayar ise kesinlikle doğrudan kapatılmamalıdır. Bilgisayarın açılması hâlinde işletim sistemi çalışacak ve bilgisayar verileri işlemeye başlayacaktır. Bunun sonucu ise, verilerin üzerine yeniden veri yazılması ve potansiyel delillerin kaybı olabilecektir. Bilgisayar açık ise kesinlikle hiçbir program çalıştırılmamalı, hatta bilgisayar kapatılmamalıdır. Herhangi bir programın çalışması, bir potansiyel delilin kaybı anlamına gelebilir. Bilgisayar çalışıyor konumda fakat ekranı siyah ise, ekranın açık olup olmadığı kontrol edilmeli, sonrasında fare (mouse) oynatılarak görüntünün gelmesi sağlanmalıdır. Çalışmakta olan bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesi, doğal olarak o anda ve olay yerinde mümkün olamayacaktır. Bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gereklidir. Kapatılması dahi veri kaybına yol açabilecek bir donanımın götürülmesi durumunda öncelikle bilgisayar üzerinde bulunan ve çalışma konumundan çıkınca yok olabilecek tüm bulgular tespit edilerek belirlenmeli, kesinlikle ekran görüntüsü fotoğraflanmalı, çalışan programlar varsa not edilmeli ve bilgisayar kapatılmayarak, arkadaki güç kablosu çekilmelidir. Bunun yapılması belki birtakım verilerin kaybına yol açabilecekse de, delillerin bütünlüğünün bozulmasının önüne geçecektir. Delillerin tümünün kaybındansa, az miktar verinin kaybı daha tercih edilir bir durumdur. Kaldı ki bilgisayardaki tüm delillere adlî bilişim uzmanlarınca ve laboratuar ortamında çeşitli analizler yapılmaksızın ulaşılması çok olası bir durum değildir. Delil araştırma amaçlı olarak yapılacak incelemeler, donanımlar üzerinde değil, alınan kopyaları üzerinde yapılmalıdır. Bu, donanımlar içerisindeki verilerin kaybını önleyecektir. Aygıtlardaki verilerin sağlıklı kopyalarının alınması çok önemlidir. Adlî bilişimde yapılan birebir kopyalama işlemine imaj (birebir kopya) denilmektedir. Bu kopyalama, sistemdeki tüm verilerin, özel yazılımlar veya donanımlar kullanmak suretiyle ve bit-bit başka bir ortamda bir örneğinin (imajının / birebir kopyasının) oluşturulması suretiyle yapılır. Adlî imajın önemi, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşma olanağını vermesidir. Sistemden imajı alınmış verilerin tümünün gözle görünür hâle getirilmesinden sonra analiz aşamasına geçilecektir. Adlî bilişimin son safhası raporlama ve yetkili makama sunma safhasıdır.

Raporlama safhası, hukuki bir değerlendirmeyi içermektedir. Değerlendirmeyi adlî bilişim uzmanı değil, kolluk yapar. Adlî bilişim uzman(lar)ının inceleme aşamasından geçmiş verilerden hangilerinin delil olabileceği, o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilir ve adlî makamlara sunulur.

4. 5651 sayılı Kanun'a göre www.abc.com, www.123.com ve www.xyz.com adlı internet sitelerinin hukukî statüsü nedir? Açıklayınız?

5651 sayılı Kanun ile içerik sağlayıcıların, yer sağlayıcıların ve erişim sağlayıcıların tanımı yapılmış ve sorumluluk ve yükümlülükleri düzenlenmiştir. **www.xyz.com** adlı arkadaşlık sitesi Amerika menşeli bir site olduğu için Türk Hukuku'na tabi olmasa da Türkiye'de ofisinin bulunması halinde 5651 sayılı Yasa'nın 2. maddesinin 1. fıkrasının m bendinde, "hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir." şeklinde tanımlandığı üzere yer sağlayıcı konumunda olacaktır. Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Yer sağlayıcı, yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, 5651 sayılı Kanunun 8'inci ve 9'uncu maddelerine göre haberdar edilmesi hâlinde ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür. 5651 sayılı Yasanın 8. maddesinin 10. fıkrasına göre, koruma tedbiri niteliğinde verilen erişime engelleme kararının varlığı hâlinde, ilgililerin hukuka uygun bir şekilde kendisine ilettiği erişim engelleme kararını teknik açıdan imkânı olduğu halde yerine getirmeyen yer sağlayıcıların sorumlularına, eylem daha ağır bir cezayı gerektirmediği takdirde altı aydan iki yıla kadar hapis cezası verilecektir. Trafik bilgisi internet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerlerin bütünüdür. Yer sağlayıcılar, trafik bilgilerini altı ay saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü tutulmuşlardır.

www.abc.com ile **www.123.com** adlı alışveriş siteleri verdikleri hizmete göre yukarıda bahsettiğimiz yer sağlayıcı ya da 5651 sayılı Yasa'nın 2. maddesinin 1. fıkrasının f bendinde düzenlenen içerik sağlayıcı olabilir. İçerik sağlayıcı ilgili maddede, "internet ortamında kullanıcılara her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir." şeklinde düzenlenmiştir. İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

5. Log kayıtlarının www.xyz.com adlı internet sitesinden temin edilmesi için hangi usulün izlenmesi gerekir, açıklayınız.

Bilişim suçlarının en önemli özelliklerinden birini de bu suçların genellikle sınır aşan bir biçimde işlenmesi ve buna bağlı olarak uluslararası bir boyutunun olmasıdır. Dolayısıyla günümüzde bilişim suçlarıyla ilgili olarak uluslararası kuruluşlar ve çalışmalar olduğu gibi, çok ciddi hukuksal düzenlemeler de bulunmaktadır. Nitekim ulusal hukuklarda konuyla ilgili olarak yapılan düzenlemelerin çoğu ya uluslararası düzenlemelerden alınmış ya da bunlara uyumlu hale getirilmiştir. Özellikle Avrupa Siber Suç Sözleşmesinin yürürlüğe girmesinden sonra taraf ülkeler için durum tam bu şekildedir. Türkiye açısından uluslararası adlî yardımlaşmaya ilişkin çok taraflı ve iki

taraflı anlaşmalar bulunmaktadır. Türkiye'nin Amerika Birleşik Devletler ile arasında ceza istinabe konusunda ikili antlaşmalar bulunmaktadır. Uluslararası istinabeye ilişkin sözleşmelerden biri de Avrupa Siber Suçlar Sözleşmesi'dir. Siber Suçlar Avrupa Sözleşmesi'ni; Amerika Birleşik Devletleri, İngiltere, Fransa, Almanya, Japonya'nın da dâhil olduğu 10 devlet imzalamış ve ulusal parlamentosunda onaylayarak yürürlüğe koymuştur. Türkiye'nin de arasında olduğu 37 ülke Sözleşmeyi imzalamış ancak henüz parlamentosundan geçirmemiştir. Sözleşme 2012 yılı Aralık ayında onay için TBMM'ye gönderilmiş, Meclis Dışişleri Komisyonunda kabul edilerek Genel Kurula sevk edilmiştir. Halen Genel Kurul gündemine alınması beklenmektedir. Siber suçlarda şüpheliye ulaşmak için en yaygın şekilde kullanılan yöntem suça konu işlem yapılırken kullanılan IP numarası tespit edilerek, IP numarasının tahsis edildiği internet abonesini belirlemektir. Bu tür suçlarla ilgili olarak yapılan uluslararası adlî yardımlaşma taleplerinin büyük çoğunluğu da IP numarası veya trafik verisinin ilgili firmadan temin edilmesi talebini içermektedir.

6. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

Bihter Zil'in Süleyman Başkol'a karşı işlemiş olduğu suç Başkasına Ait Banka Kartının Ele Geçirilmesi veya Elde Bulundurulması Suçu Soruşturması

a) Şikâyetçi Süleyman Başkol'a ait Zakkum Bankası'ndan alınan banka kartına ait söz konusu harcamaları gösteren hesap dökümünün okunaklı bir şekilde talebi.

b) Zakkum Bankası'nın şubesinden varsa güvenlik kamerası görüntüleri talebi.

c) Banka kartının ele geçirilmesi akabinde kartla herhangi bir işlem yapılıp yapılmadığının tespitini içeren hesap dökümünün Zakkum Bankasından talebi.

d) Banka kartıyla alışveriş yapılmış olduğunun tespiti hâlinde, alışveriş yapılan şirket yetkilerinin konuyla ilgili ifade sahibi, sıfatıyla alışverişi kimin yaptığı, bu konunun tespitine ilişkin tüm bilgi ve belgelerin elde edilmesi için beyanının alınması (IP numarası, telefon numarası, kimlik ve adres, ürünün teslim yeri ve adresi)

e) Şirketten elde edilecek bilgilerden, kamera görüntülerinden ve hesap dökümanlarından yola çıkılarak söz konusu alışverişleri yapan internet abonesinin tespiti için Telekom Müdürlüğü veya diğer servis sağlayıcılardan gerekli bilgi ve belgelerin elde edilmesi,

f) Bu şekilde şüpheliye ulaşılması,

g) Şüphelinin müdafili savunmasının alınması.

Bihter Zil'in "Sahte Oluşturulan Veya Üzerinde Sahtecilik Yapılan Bir Bank Kartını Kullanmak Suretiyle Kendisine Veya Başkasına Yarar Sağlama Suçunun" Soruşturulması

a) Şikâyetçi Süleyman Başkol'a ait Zakkum Bankası'ndan alınan banka kartına ait söz konusu harcamaları gösteren hesap dökümünün okunaklı bir şekilde talebi.

b) Harcamanın ne şekilde yapıldığının Z bankasından sorulması (POS/ internet)

c) İnternet üzerinden yapılmış ise hangi IP numaradan hangi tarih ve saat aralığında yapıldığı nın Banka'dan sorulması.

d) POS cihazından yapılmış ise hangi işyerine ait POS cihazından yapıldığının Banka'dan sorulması. (iş yerinin açık unvan, adres ve telefonu)

e) Şikâyetçinin kartının hala kullanımda olup olmadığının Banka'dan sorulması.

f) Şikâyetçinin Zakkum Bankası'na herhangi bir müracaatının bulunup bulunmadığının Bankadan sorulması,

g) Şikâyetçinin müracaatının olması durumunda ne gibi bir işlem yapıldığının sorulması,

h) Alışveriş yapılan şirket yetkilerinin konuyla ilgili ifade sahibi, sıfatıyla alışverişi kimin yaptığı, bu konunun tespitine ilişkin tüm bilgi ve belgelerin elde edilmesi için beyanının alınması (IP numarası, telefon numarası, kimlik ve adres, ürünün teslim yeri ve adresi)

ı) Şirketten elde edilecek bilgilerden yola çıkılarak söz konusu alışverişleri yapan internet abonesinin tespiti için Telekom Müdürlüğü veya diğer servis sağlayıcılardan gerekli bilgi ve belgelerin elde edilmesi,

i) Bu şekilde şüpheliye ulaşılması,

j) Şüphelinin müdafili savunmasının alınması.

Bihter Zil'in Selin Kaptı'ya karşı "nitelikli hırsızlık suçunun" soruşturması

a) Selin Kaptı'nın Zakkum Bankası X şubesindeki hesabından söz konusu internet havalesini yapan abonenin tespiti için, havaleyi yapan abonenin IP numarasının ve abonenin tespitine yarayan diğer bilgilerin Banka Şubesi'nden alınması.

b) IP numarası ve benzeri bilgilerin kime ait olduğunun Telekom Müdürlüğü veya diğer şirketler aracılığı ile tespit edilerek bu şahsın CMK 147 maddesi ve devamı maddeleri gereğince müdafili savunmalarının alınması,

c) Zakkum Bankası X şubesinden, Bihter Zil'in hesap numarası, adres ve kimlik tespitine ilişkin tüm bilgi ve belgelerin varsa güvenlik kamerasından görüntülerin de alınarak bu şahsın tespiti ile 147 vd. maddeleri gereğince savunmalarının alınması.

ZAKKUM BANK

Hesap Adı: Selin Kaptı

Hesap Tipi: Cari Hesap

Hesap Tarihi: 11 Aralık 2013

Hesap Şubesi: Şaşkınbakkal

Hesap Numarası: 1234 3245 1354

Sayfa:1

Tarih	İşlem Türü	Açıklama	Ödenen	Bakiye
11.Ara.13		Açılış Bakiyesi		125.000,00 TL
02.Ocak.14	ATM	Para çekimi	700,00 TL	124.300,00 TL
04. Ocak 14	ATM	Para çekimi	500,00 TL	123.800,00 TL
05. Ocak 14	EFT	TR 43 6758 5467 4358 IBAN numarasına para gönderimi Para gönderimi	50,00 TL	123.750,00 TL
08. Ocak 14	Havale	TR 57 8976 5647 3455 7869 IBAN numarasına para gönderimi	150,00 TL	123.600,00 TL
10. Ocak 14	ATM	Para çekimi	200,00 TL	123.400,00 TL
13. Ocak 14	EFT	TR 34 6786 4567 9807 IBAN numarasına para gönderimi	100,00 TL	123.300,00 TL
14. Ocak 14	Havale	TR 57 8976 5647 3455 7869 IBAN numarasına Para gönderimi	25,00 TL	123.275,00 TL
18. Ocak 14	ATM	Para çekimi	100,00 TL	123.175,00 TL
20. Ocak 14	ATM	Para çekimi	250,00 TL	122.925,00 TL
22. Ocak.14	EFT	TR 43 6758 5467 4358 IBAN numarasına para gönderimi	250,00 TL	122.675,00 TL
25.Ocak.14	ATM	Para çekimi	500,00 TL	122.175,00 TL
26. Ocak 14	Havale	TR 57 8976 5647 3455 7869 IBAN numarasına para gönderimi	200,00 TL	121.975,00 TL
29. Ocak 14	ATM	Para çekimi	300,00 TL	121.675,00 TL
31. Ocak.14	EFT	TR 56 0001 0024 6102 IBAN numarasına para gönderimi	100.000,00 TL	21.525,00 TL

Bilgileriniz

Müşteri Numarası	456893473
Kart Numarası	5157 743587565235
Kart Limiti	1.000,00 TL
Ekspres Limit	2.000,00 TL
Nakit Avans Limiti	750,00 TL
Hesap Kesim Tarihi	6.12.2013
Son Ödeme Tarihi	13.12.2013
Toplam Borcunuz	1.000,00 TL
Min. Ödeme Tutarı	200,00 TL

Süleyman Başkol

Namık Bey Mahallesi
Altın Sokak
No:14
Posta Kodu: 43256
İl/İlçe: İstanbul/ Altunizade

Son ödeme tarihi: 13.12.2013

İşlem tarihi	Dönem içi işlemler	Kalan Borç/ Taksit	Bonus(TL)	İşlem Tutarı
YAPTIĞINIZ HARCAMALAR				**TL**
6.11.2013	AREZTEK.NET Arezandland.com			150,00
10.11.2013	SAVAVARTEKSTİL			100,00
15.11.2013	ABCGİYİMTEKSİT.AŞ. www.abc.com			250,00
17.11.2013	123jeangiyim A.Ş. www.123.com			300,00
20.11.2013	xyzfriendssearch.net www.xyz.com			150,00
29.11.2013	software.net www.software23.com			50,00
Toplam				**1.000,00 TL**

Hesap Özeti

(+)Önceki Hesap Bakiyeniz	
(+)Dönem içi harcamanız	
(+)Toplam faiz ve ücretler	
(+)Ödemeler	
(=)Toplam Borcunuz	
Min. Ödeme Tutarı	200,00TL

BU DÖNEM UYGULANAN AYLIK FAİZ ORANI

Alışveriş Faiz Oranı	%8
Nakit Avan Faiz Oranı	%5
Gecikme Faiz Oranı	%12

GELECEK DÖNEM EKSTRE BİLGİNİZ

Bir Sonraki Ay Hesap Kesim Tarihi	6.1.2014
Bir Sonraki Ay Son Ödeme Tarihi	12.1.2014

Vaka Analizi 3

Texil, tekstil ürünleri satan ve alanında öncü olan bir e-ticaret firmasıdır. Serverm ise Texil şirketine 5 yıldır servis sağlayıcılığı hizmeti vermektedir. Texil, bu hizmeti karşılığında Serverm'e her ay 30.000 TL ödemektedir. 5. Yılın sonunda, Texil'ye diğer servis sağlayıcı firmalardan uygun tekliflerin gelmesi üzerine Serverm'e durumu bildirip ücreti düşürmemeleri hâlinde başka firmalar ile anlaşılacağını belirtmiştir. Gelirinin büyük bir bölümünü Texil şirketinden sağlayan Serverm, bu konuda birçok teklif hazırlayıp, Texil şirket genel müdürü Rafi Manger'e sunmuştur. Ancak tekliflerden tatmin olmayan Texil, Serverm ile anlaşmasını sona erdirerek Giyote adlı yeni bir servis sağlayıcı firma ile sözleşme imzalamıştır.

Bütün çabalarına rağmen Texil'in Giyote ile anlaşmasına sinirlenen ve gelirinin büyük bir bölümünü kaybeden Serverm genel müdürü Yaşar Kaybetmez, şirketin IT çalışanı Mazlum Münir'e " Onlara göster gününü, sen ne yapacağını bilirsin!" şeklinde bir mail atmıştır.

Şirket çalışanı Mazlum Münir, Yaşar Kaybetmez'den almış olduğu mail üzerine alışverişin en yoğun olduğu saatlerde 2 ay boyunca birçok makine üzerinden Texil şirketinin yeni serverlarına saldırı yaparak hedef sistemin kimseye hizmet veremez hâle gelmesine neden olmuştur.

Texil şirketinin yeni servis sağlayıcı firması Giyote durumu ilk anda fark etmiş olsa da bahsi geçen saldırıları engelleyememiştir. Bu durumun 2 ay boyunca şiddetli bir şekilde devam etmesi üzerine mağdur olan Texil şirketi genel müdürü Rafi Manger, savcılığa giderek suç duyurusunda bulunmuştur.

SORULAR

1. Mazlum Münir'in Texil şirketinin serverlarına karşı gerçekleştirmiş olduğu saldırıda hangi teknik yöntem kullanılmıştır, açıklayınız.
2. Olaydaki suç tiplerini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.
3. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.
4. 5651 sayılı Kanun'a göre Texil'in e-ticaret firmasının hukuki statüsü nedir, açıklayınız.
5. Texil'in e-ticaret firması yabancı menşeli bir firma olsaydı, log kayıtlarının temin edilmesi için hangi usulün izlenmesi gerektiğini açıklayınız.
6. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

CEVAPLAR

1. Mazlum Münir'nin Texil şirketinin serverlarına karşı gerçekleştirmiş olduğu saldırıda hangi teknik yöntem kullanılmıştır, açıklayınız.

Bu saldırıda DDOS tekniği kullanılmıştır.

Dos; yani açılımı Denial of Sevice olan bu saldırı çeşidi bir hizmet aksatma yöntemidir. Bir kişinin bir sisteme düzenli veya arka arkaya yaptığı saldırılar sonucunda hedef sistemin kimseye hizmet veremez hâle gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlayan bir saldırı çeşididir. Birçok Yöntemle Hizmet aksatma saldırıları gerçekleştirilebilir.

DDos ise; bir saldırganın daha önceden tasarladığı birçok makine üzerinden hedef bilgisayara saldırı yaparak hedef sistemin kimseye hizmet veremez hâle gelmesini amaçlayan bir saldırı çeşididir. Koordineli olarak yapılan bu işlem hem saldırının boyutunu artırır hem de saldırıyı yapan kişinin gizlenmesini sağlar. Bu işlemleri yapan araçlara Zombi denir. Bu saldırı çeşidinde saldırganı bulmak zorlaşır. Çünkü saldırının merkezinde bulunan saldırgan aslında saldırıya katılmaz. Sadece diğer ip numaralarını yönlendirir. Eğer saldırı bir tek ip adresinden yapılırsa bir Firewall bunu rahatlıkla engelleyebilir. Fakat saldırı daha yüksek sayıdaki ip adresinden gelmesi Firewall un devre dışı kalmasını sağlar (Log taşması firewall servislerini durdurur). İşte bu özelliği onu DoS sadırısından ayıran en önemli özelliğidir.

2. Olaydaki suç tiplerini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.

Serverm genel müdürü Yaşar Kaybetmez azmettiren sıfatıyla, şirketin IT çalışanı Mazlum Münir fail sıfatıyla Texil şirketine karşı bilişim sistemini engellemek suretiyle TCK 244/1 "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu" işlemiştir.

3. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.

Şüphelinin tespit edilmesinden sonra başkaca bir suretle delil elde edilmesinin mümkün olmaması nedeniyle, CMK madde 134'e göre Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına hâkim tarafından karar verilir. Delillerin sağlıklı biçimde toplanabilmesi, olay yerine yapılan ilk müdehalenin ne kadar sağlıklı olduğuna bağlıdır. Adlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde edilirken bilgisayardaki verilerin mevcut hali ile yedeği alınmalı, bilgisayar iade edilmeli ve yapılacak arama işlemi bu yedek üzerinde yapılmalıdır. Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifre çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar gecikme olmaksızın iade edilir. Şüphelinin bilgisayarında bizzat bulundurulması suç olan kredi kartı şifreleri, çocuk pornografisi vb. mevcut ise yedeklerin verilmemesi gerekmektedir. Çıkartılacak yedekten şüpheliye veya vekiline örnek verilmesi bu kişilerin isteğine bırakılmıştır. Ancak şüpheliye örnek isteyip istemediği sorulup bu husus kayıt altına alınmalıdır. Delil toplamadaki başarı oranı, bilişim suçlarıyla mücadelenin önemli bir göstergesidir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz saptanması ve zarar görmeden toplanması, ilk olay yeri müdehalesinin düzgün yapılmasıyla mümkündür. Adlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde etme çalışması sırasında, olay

yerinde varsa (örneğin güvenliği sağlayan) konu hakkında bilgi ve tecrübesi olmayan kişilerin aygıt ve sisteme müdehaleleri kesinlikle engellenmelidir. Kriminal inceleme yürütülürken elektronik deliller de toplanmalı, bunun için öncelikle delillerin nerede ve hangi formatta olduğu, nasıl depolandığı tespit edilmelidir. Sonrasında, ortamda bulunan elektronik donanımların çalışma biçimleri ve birbirlerine bağlılıkları tespit edilerek buna göre hareket edilir. Örneğin, olay yerinde kapalı konumda bulunan bir bilgisayar varsa kesinlikle açılmamalı; açık bir bilgisayar ise kesinlikle doğrudan kapatılmamalıdır. Bilgisayarın açılması hâlinde işletim sistemi çalışacak ve bilgisayar verileri işlemeye başlayacaktır. Bunun sonucu ise, verilerin üzerine yeniden veri yazılması ve potansiyel delillerin kaybı olabilecektir. Bilgisayar açık ise kesinlikle hiçbir program çalıştırılmamalı, hatta bilgisayar kapatılmamalıdır. Herhangi bir programın çalışması, bir potansiyel delilin kaybı anlamına gelebilir. Bilgisayar çalışıyor konumda fakat ekranı siyah ise, ekranın açık olup olmadığı kontrol edilmeli, sonrasında fare (mouse) oynatılarak görüntünün gelmesi sağlanmalıdır. Çalışmakta olan bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesi, doğal olarak o anda ve olay yerinde mümkün olamayacaktır. Bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gereklidir. Kapatılması dahi veri kaybına yol açabilecek bir donanımın götürülmesi durumunda öncelikle bilgisayar üzerinde bulunan ve çalışma konumundan çıkınca yok olabilecek tüm bulgular tespit edilerek belirlenmeli, kesinlikle ekran görüntüsü fotoğraflanmalı, çalışan programlar varsa not edilmeli ve bilgisayar kapatılmayarak, arkadaki güç kablosu çekilmelidir. Bunun yapılması belki birtakım verilerin kaybına yol açabilecekse de, delillerin bütünlüğünün bozulmasının önüne geçecektir. Delillerin tümünün kaybındansa, az miktar verinin kaybı daha tercih edilir bir durumdur. Kaldı ki bilgisayardaki tüm delillere adlî bilişim uzmanlarınca ve laboratuar ortamında çeşitli analizler yapılmaksızın ulaşılması çok olası bir durum değildir. Delil araştırma amaçlı olarak yapılacak incelemeler, donanımlar üzerinde değil, alınan kopyaları üzerinde yapılmalıdır. Bu, donanımlar içerisindeki verilerin kaybını önleyecektir. Aygıtlardaki verilerin sağlıklı kopyalarının alınması çok önemlidir. Adlî bilişimde yapılan birebir kopyalama işlemine imaj (birebir kopya) denilmektedir. Bu kopyalama, sistemdeki tüm verilerin, özel yazılımlar veya donanımlar kullanmak suretiyle ve bit-bit başka bir ortamda bir örneğinin (imajının / birebir kopyasının) oluşturulması suretiyle yapılır. Adlî imajın önemi, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşma olanağını vermesidir. Sistemden imajı alınmış verilerin tümünün gözle görünür hâle getirilmesinden sonra analiz aşamasına geçilecektir. Adlî bilişimin son safhası raporlama ve yetkili makama sunma safhasıdır. Raporlama safhası, hukuki bir değerlendirmeyi içermektedir. Değerlendirmeyi adlî bilişim uzmanı değil, kolluk yapar. Adlî bilişim uzman(lar)ının inceleme aşamasından geçmiş verilerden hangilerinin delil olabileceği, o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilir ve adlî makamlara sunulur.

4. 5651 sayılı Kanun'a göre Texil'in e-ticaret firmasının hukuki statüsü nedir, açıklayınız.

Texil'in e-ticaret firması verdikleri hizmete göre yer sağlayıcı ya da içerik sağlayıcı olabilir.

Yer sağlayıcı; 5651 sayılı Yasa'nın 2. maddesinin 1. fıkrasının m bendinde, "hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir." şeklinde tanımlandığı üzere yer sağlayıcı olarak tanımlanmıştır. Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Yer sağlayıcı, yer sağladığı

hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, 5651 sayılı Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür. 5651 sayılı Yasanın 8. maddesinin 10. fıkrasına göre, koruma tedbiri niteliğinde verilen erişime engelleme kararının varlığı hâlinde, ilgililerin hukuka uygun bir şekilde kendisine ilettiği erişim engelleme kararını teknik açıdan imkânı olduğu hâlde yerine getirmeyen yer sağlayıcıların sorumlularına, eylem daha ağır bir cezayı gerektirmediği takdirde altı aydan iki yıla kadar hapis cezası verilecektir. Trafik bilgisi internet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerlerin bütünüdür. Yer sağlayıcılar, trafik bilgilerini altı ay saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü tutulmuşlardır.

İçerik sağlayıcı; 5651 sayılı Yasa'nın 2. maddesinin 1. fıkrasının f bendinde, "internet ortamında kullanıcılara her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir." şeklinde düzenlenmiştir. İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

5. Texil'in e-ticaret firması yabancı menşeli bir firma olsaydı, log kayıtlarının temin edilmesi için hangi usulün izlenmesi gerektiğini açıklayınız.

Bilişim suçlarının en önemli özelliklerinden birini de bu suçların genellikle sınır aşan bir biçimde işlenmesi ve buna bağlı olarak uluslararası bir boyutunun olmasıdır. Dolayısıyla günümüzde bilişim suçlarıyla ilgili olarak uluslararası kuruluşlar ve çalışmalar olduğu gibi, çok ciddi hukuksal düzenlemeler de bulunmaktadır. Nitekim ulusal hukuklarda konuyla ilgili olarak yapılan düzenlemelerin çoğu ya uluslararası düzenlemelerden alınmış ya da bunlara uyumlu hâle getirilmiştir. Özellikle Avrupa Siber Suç Sözleşmesinin yürürlüğe girmesinden sonra taraf ülkeler için durum tam bu şekildedir. Türkiye açısından uluslararası adlî yardımlaşmaya ilişkin çok taraflı ve iki taraflı anlaşmalar bulunmaktadır. Türkiye'nin Amerika Birleşik Devletler ile arasında ceza istinabe konusunda ikili antlaşmalar bulunmaktadır. Uluslararası istinabeye ilişkin sözleşmelerden biri de Avrupa Siber Suçlar Sözleşmesi'dir. Siber Suçlar Avrupa Sözleşmesi'ni; Amerika Birleşik Devletleri, İngiltere, Fransa, Almanya, Japonya'nın da dâhil olduğu 10 devlet imzalamış ve ulusal parlamentosunda onaylayarak yürürlüğe koymuştur. Türkiye'nin de arasında olduğu 37 ülke Sözleşmeyi imzalamış ancak henüz parlamentosundan geçirmemiştir. Sözleşme 2012 yılı Aralık ayında onay için TBMM'ye gönderilmiş, Meclis Dışişleri Komisyonunda kabul edilerek Genel Kurula sevk edilmiştir. Hâlen Genel Kurul gündemine alınması beklenmektedir. Siber suçlarda şüpheliye ulaşmak için en yaygın şekilde kullanılan yöntem suça konu işlem yapılırken kullanılan IP numarası tespit edilerek, IP numarasının tahsis edildiği internet abonesini belirlemektir. Bu tür suçlarla ilgili olarak yapılan uluslararası adlî yardımlaşma taleplerinin büyük çoğunluğu da IP numarası veya trafik verisinin ilgili firmadan temin edilmesi talebini içermektedir.

6. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

a) Texil şirketinin yer sağlayıcısı olan Giyote hosting şirketinden saldırıların gerçekleştiği tarihlerde söz konusu siteleri ziyaret eden IP numaraları talep edilir.

b) Tespit edilen IP numaraları kullanılan şahıs telefon, adres ve kimlik bilgilerinin Türk Telekom veya diğer servis sağlayıcılardan sorulur. Son 3 aylık uygulamada; TİB'in yetkilendirmiş olduğu Emniyet Müdürlüğü'nde bulunan birim sayesinde şüphelinin IP adresini tespit için servis sağlayıcılara yazı yazma gereksinimi sona ermiştir. Söz konusu birim, çok daha kısa bir süre içinde şüphelinin IP bilgilerini tespit edebilmektedir.

c) İlgili firma ve kuruluşlardan gönderilen kimlik ve adres bilgisi kontrol edilerek şüpheli şahıs ya da şahıslar tespit edilir.

d) Savcılığın talimatı doğrultusunda başka suç ve suç delillerinin elde edilebilmesi amacıyla şüpheli şahsın ikametine veya işyerine arama, el koyma ayrıca arama sonucu elde edilecek olan bilgisayar ve diğer dijital materyaller üzerinde CMK'nın 134. Maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde, hard disklerinde arama, inceleme, izin talebinde bulunulur.

e) Arama esnasında tespit edilen dijital materyallerin imajlarının alınarak incelenmesinde kullanılmak üzere ilgili Cumhuriyet Savcılığı'ndan el konulan materyallerin %30 fazlası hard disk fazlası talebinde bulunulur.

f) Tespit edilen dijital materyaller üst yazı ile içeriğinde inceleme izni bulunan mahkeme kararı ve soruşturma evrakının bir örneği ile Siber Suçlarla Mücadele Şube Müdürlüğü'ne elden teslim edilir.

g) İnceleme sonucunda hazırlanan rapor ve dijital materyaller soruşturma birimince teslim alınır.

h) Rapor ve diğer deliller doğrultusunda suçla ilgili şüpheli şahsın konu hakkında ayrıntılı ifadesi alınır.

VAKA ANALİZİ 4

Cizgifilmilehayat.com alan adlı site; çocukların sıklıkla ziyaret ederek istedikleri çizgi filmleri izledikleri çocuklara özgü bir internet sitesidir. Bu sitenin sahibinin arkadaşından aldığı USB'den ücretsiz programı bilgisayarına kaydetmesiyle, bilgisayara zararlı yazılım yüklenmiştir. Bu zararlı yazılım, Coşkun Sapkın tarafından üretilmiştir. Bu zararlı yazılım sayesinde Coşkun Sapkın, sitede kayıtlı bazı çizgi film videolarını değiştirerek belli bir dakikadan sonra bu videolara cinsel içerikli görüntüler yerleştirmiştir. Çizgi film izlemek için siteyi ziyaret eden 6 yaşındaki Çisem Çaresiz, içeriği değiştirilmiş videoları ailesine hiçbir şey söylemeyerek izlemeye devam etmiştir.

Atıl anaokulunda okuyan kız çocuğu Çisem Çaresiz, izlediği çizgi filmlerde değişik şeyler gördüğünü ve anlam veremediğini bale öğretmeni Hasan Münasebetsiz'e anlatmış ve bu çizgi film videolarını izletmiştir. Hasan Münasebetsiz, videolardaki kişilerin oyun oynadıklarını ve çok eğlendiklerini, eğer isterse kendisinin de bu oyunu oynayarak videolarda yer alabileceğini söylemiştir. Çisem Çaresiz'nin "oyun oynamayı" kabul etmesi üzerine, Hasan Münasebetsiz bu oyun videolarından ailesine bahsetmemesini, onlara sürpriz hazırlayacaklarını söyleyerek Çisem Çaresiz'i tembihlemiştir. Sonrasında Hasan Münasebetsiz, Çisem Çaresiz'i birçok cinsel içerikli videoda oynatmış ve bu videoları porno sitelerinde paylaşmıştır.

Çisem Çaresiz'nin 21 yaşındaki kuzeni Kaan Bostan, Hasan Münasebetsiz'in videoları yüklediği sitelerden birine üye olup ücretini ödeyerek birçok videoyu bilgisayarına indirmiştir. İndirdiği videolarda kuzeni Çisem Çaresiz'in oynadığını görüp panik içinde ailesine haber vermiştir.

Çisem Çaresiz'in ailesi, videoları izlemelerinin hemen ardından Savcılığa suç duyurusunda bulunmuştur.

SORULAR

1. Coşkun Sapkın cizgifilmilehayat.com sitesine zararlı yazılım yüklemek için hangi teknik yöntemi kullanılmıştır, açıklayınız.
2. Olaydaki suç tiplerini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.
3. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, Kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.
4. 5651 sayılı Kanun'a göre Cizgifilmilehayat.com adlı sitenin hukukî statüsü nedir? Açıklayınız.
5. Cizgifilmilehayat.com yabancı menşeli olsaydı, log kayıtlarının temin edilmesi için hangi usulün izlenmesi gerektiğini açıklayınız.
6. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

CEVAPLAR

1. Coşkun Sapkın cizgifilmilehayat.com sitesine zararlı yazılım yüklemek için hangi teknik yöntemi kullanılmıştır, açıklayınız.

Coşkun Sapkın cizgifilmilehayat.com sitesine zararlı yazılım yüklemek için

kullanmış olduğu teknik yöntem "Truva atıdır (trojan). Truva atı; yararlı gibi görünen ancak aslında zarara yol açan bilgisayar programlarıdır. Truva atları, insanların, meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya yöneltilmeleri yoluyla yayılır. Truva atları, ücretsiz olarak yüklediğiniz yazılımlarda da bulunabilir. Güvenmediğiniz bir kaynaktan asla yazılım yüklemeyin.

Trojan "kurban"ının tahmin etmediği bir şekilde ve isteği olmaksızın, gizli ve genellikle kötü amaçlı bir faaliyette bulunan bir programdır. Virüsten farkı kendi kendini çoğaltmamasıdır (her ne kadar bu ayrım evrensel olarak kabul görmemişse de).

2. Olaydaki suç tiplerini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir? Açıklayınız.

Coşkun Sapkın, **www.cizgifilmilehayat.com** sitesini hackleyip video içeriklerini (verileri) değiştirmek suretiyle "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme suçunu" işlemiştir.

Coşkun Sapkın'ın söz konusu sitedeki videolara müstehcen görüntüler ekleme fiili, TCK 226/1-b'de düzenlenen" içeriklerin çocukların girebileceği veya çocukların görebileceği yerlerde alenen göstermek" suretiyle işlenen müstehcenlik suçu kapsamındadır. Buna ilaveten söz konusu fiil aynı zamanda 226/2'de düzenlenen "müstehcen görüntülerin basın ve yayın yoluyla yayınlanması" suçunu oluşturmaktadır. Bu durum TCK madde 44'te düzenlenen "fikri içtima" kapsamında değerlendirileceğinden, Coşkun Sapkın, daha ağır cezayı gerektiren TCK madde 226/2'den dolayı cezalandırılacaktır.

Hasan Münasebetsiz'in küçük Çisem Çaresiz'i cinsel içerikli videolarda oynatma eylemi, TCK m. 226/3'te düzenlenen müstehcen görüntü içeren ürünlerin üretiminde çocukların kullanılması suçunu oluşturmaktadır. Aynı zamanda Hasan Münasebetsiz'in bu videoları porno sitesinde yayınlama fiili "ürünlerin içeriğini basın ve yayın yoluyla yayma" suçunu (TCK m. 226/5) oluşturmaktadır. Bu içerikleri basın ve yayın yoluyla kullanıma sunulması Hasan Münasebetsiz tarafından gerçekleştirilen eylemler birbirinden farklı iki ayrı suç oluşturduğundan gerçek içtima uygulanacaktır.

Kaan Bostan'ın porno sitesinden "çocuk pornosu indirmek suretiyle" bu içerikleri bilgisayarında bulundurması TCK 226/3'teki "çocuk pornosu bulundurma" suçunu oluşturmaktadır.

3. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.

Şüphelinin tespit edilmesinden sonra başkaca bir suretle delil elde edilmesinin mümkün olmaması nedeniyle, CMK madde 134'e göre Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına hâkim tarafından karar verilir. Delillerin sağlıklı biçimde toplanabilmesi, olay yerine yapılan ilk müdahalenin ne kadar sağlıklı olduğuna bağlıdır. Adlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde edilirken bilgisayardaki verilerin mevcut hâli ile yedeği alınmalı, bilgisayar iade edilmeli

ve yapılacak arama işlemi bu yedek üzerinde yapılmalıdır. Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifre çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar gecikme olmaksızın iade edilir. Şüphelinin bilgisayarında bizzat bulundurulması suç olan kredi kartı şifreleri, çocuk pornografisi vb. mevcut ise yedeklerin verilmemesi gerekmektedir. Çıkartılacak yedekten şüpheliye veya vekiline örnek verilmesi bu kişilerin isteğine bırakılmıştır. Ancak şüpheliye örnek isteyip istemediği sorulup bu husus kayıt altına alınmalıdır. Delil toplamadaki başarı oranı, bilişim suçlarıyla mücadelenin önemli bir göstergesidir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz saptanması ve zarar görmeden toplanması, ilk olay yeri müdahalesinin düzgün yapılmasıyla mümkündür. Adlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde etme çalışması sırasında, olay yerinde varsa (örneğin güvenliği sağlayan) konu hakkında bilgi ve tecrübesi olmayan kişilerin aygıt ve sisteme müdahaleleri kesinlikle engellenmelidir. Kriminal inceleme yürütülürken elektronik deliller de toplanmalı, bunun için öncelikle delillerin nerede ve hangi formatta olduğu, nasıl depolandığı tespit edilmelidir. Sonrasında, ortamda bulunan elektronik donanımların çalışma biçimleri ve birbirlerine bağlılıkları tespit edilerek buna göre hareket edilir. Örneğin, olay yerinde kapalı konumda bulunan bir bilgisayar varsa kesinlikle açılmamalı; açık bir bilgisayar ise kesinlikle doğrudan kapatılmamalıdır. Bilgisayarın açılması hâlinde işletim sistemi çalışacak ve bilgisayar verileri işlemeye başlayacaktır. Bunun sonucu ise, verilerin üzerine yeniden veri yazılması ve potansiyel delillerin kaybı olabilecektir. Bilgisayar açık ise kesinlikle hiçbir program çalıştırılmamalı, hatta bilgisayar kapatılmamalıdır. Herhangi bir programın çalışması, bir potansiyel delilin kaybı anlamına gelebilir. Bilgisayar çalışıyor konumda fakat ekranı siyah ise, ekranın açık olup olmadığı kontrol edilmeli, sonrasında fare (mouse) oynatılarak görüntünün gelmesi sağlanmalıdır. Çalışmakta olan bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesi, doğal olarak o anda ve olay yerinde mümkün olamayacaktır. Bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gereklidir. Kapatılması dahi veri kaybına yol açabilecek bir donanımın götürülmesi durumunda öncelikle bilgisayar üzerinde bulunan ve çalışma konumundan çıkınca yok olabilecek tüm bulgular tespit edilerek belirlenmeli, kesinlikle ekran görüntüsü fotoğraflanmalı, çalışan programlar varsa not edilmeli ve bilgisayar kapatılmayarak, arkadaki güç kablosu çekilmelidir. Bunun yapılması belki birtakım verilerin kaybına yol açabilecekse de, delillerin bütünlüğünün bozulmasının önüne geçecektir. Delillerin tümünün kaybındansa, az miktar verinin kaybı daha tercih edilir bir durumdur. Kaldı ki, bilgisayardaki tüm delillere adlî bilişim uzmanlarınca ve laboratuar ortamında çeşitli analizler yapılmaksızın ulaşılması çok olası bir durum değildir. Delil araştırma amaçlı olarak yapılacak incelemeler, donanımlar üzerinde değil, alınan kopyaları üzerinde yapılmalıdır. Bu, donanımlar içerisindeki verilerin kaybını önleyecektir. Aygıtlardaki verilerin sağlıklı kopyalarının alınması çok önemlidir. Adlî bilişimde yapılan birebir kopyalama işlemine imaj (birebir kopya) denilmektedir. Bu kopyalama, sistemdeki tüm verilerin, özel yazılımlar veya donanımlar kullanmak suretiyle ve bit-bit başka bir ortamda bir örneğinin (imajının / birebir kopyasının) oluşturulması suretiyle yapılır. Adlî imajın önemi, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşma olanağını vermesidir. Sistemden imajı alınmış verilerin tümünün gözle görünür hale getirilmesinden sonra analiz aşamasına geçilecektir. Adlî bilişimin son safhası raporlama ve yetkili makama sunma safhasıdır. Raporlama safhası, hukuki bir değerlendirmeyi içermektedir. Değerlendirmeyi adlî bilişim uzmanı değil, kolluk yapar. Adlî bilişim uzman(lar)ının inceleme aşamasından

geçmiş verilerden hangilerinin delil olabileceği, o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilir ve adlî makamlara sunulur.

4. 5651 sayılı Kanun'a göre Cizgifilmilehayat.com adlı sitenin hukuki statüsü nedir? Açıklayınız.

5651 sayılı Yasa'nın 2. maddesinin 1. fıkrasının f bendinde düzenlenen içerik sağlayıcılardır. İçerik sağlayıcı ilgili maddede, "internet ortamında kullanıcılara her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir." şeklinde düzenlenmiştir. İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

5. Cizgifilmilehayat.com yabancı menşeli olsaydı, log kayıtlarının temin edilmesi için hangi usulün izlenmesi gerektiğini açıklayınız.

Bilişim suçlarının en önemli özelliklerinden birini de bu suçların genellikle sınır aşan bir biçimde işlenmesi ve buna bağlı olarak uluslararası bir boyutunun olmasıdır. Dolayısıyla günümüzde bilişim suçlarıyla ilgili olarak uluslararası kuruluşlar ve çalışmalar olduğu gibi, çok ciddi hukuksal düzenlemeler de bulunmaktadır. Nitekim ulusal hukuklarda konuyla ilgili olarak yapılan düzenlemelerin çoğu ya uluslararası düzenlemelerden alınmış ya da bunlara uyumlu hale getirilmiştir. Özellikle Avrupa Siber Suç Sözleşmesinin yürürlüğe girmesinden sonra taraf ülkeler için durum tam bu şekildedir. Türkiye açısından uluslararası adlî yardımlaşmaya ilişkin çok taraflı ve iki taraflı anlaşmalar bulunmaktadır. Türkiye'nin Amerika Birleşik Devletler ile arasında ceza istinabe konusunda ikili antlaşmalar bulunmaktadır. Uluslararası istinabeye ilişkin sözleşmelerden biri de Avrupa Siber Suçlar Sözleşmesi'dir. Siber Suçlar Avrupa Sözleşmesi'ni; Amerika Birleşik Devletleri, İngiltere, Fransa, Almanya, Japonya'nın da dâhil olduğu 10 devlet imzalamış ve ulusal parlamentosunda onaylayarak yürürlüğe koymuştur. Türkiye'nin de arasında olduğu 37 ülke Sözleşmeyi imzalamış ancak henüz parlamentosundan geçirmemiştir. Sözleşme 2012 yılı Aralık ayında onay için TBMM'ye gönderilmiş, Meclis Dışişleri Komisyonunda kabul edilerek Genel Kurula sevk edilmiştir. Halen Genel Kurul gündemine alınması beklenmektedir. Siber suçlarda şüpheliye ulaşmak için en yaygın şekilde kullanılan yöntem suça konu işlem yapılırken kullanılan IP numarası tespit edilerek IP numarasının tahsis edildiği internet abonesini belirlemektir. Bu tür suçlarla ilgili olarak yapılan uluslararası adlî yardımlaşma taleplerinin büyük çoğunluğu da IP numarası veya trafik verisinin ilgili firmadan temin edilmesi talebini içermektedir.

6. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

Coşkun Sapkın'ın "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçunun Soruşturulması"

a) Müşteki savcılık makamından havaleli dilekçe ile birlikte İlçe Emniyet Müdürlüğüne gelir.

b) Müştekinin dilekçedeki/savcılık ifadesindeki bilgiler yeterli değilse ayrıntılı ifadesi alınır.

c)Site ile ilgili internet üzerinden **www.tib.gov.tr** adresinden whois sorgusu yapılır.

d)Site hakkında web tespit raporu tanzim edilir.

e) Hacklenen internet sitesine giriş yapılan bilgisayarın IP numaraları sitenin hosting firmasından (yer sağlayıcı) talep edilir.

f) Şüpheli IP adresi servis sağlayıcıdan (Türk Telekom'dan) sorulur. Son 3 aylık uygulamada; TİB'in yetkilendirmiş olduğu Emniyet Müdürlüğü'nde bulunan birim sayesinde şüphelinin IP adresini tespit için servis sağlayıcılara yazı yazma gereksinimi sona ermiştir. Söz konusu birim, çok daha kısa bir süre içinde şüphelinin IP bilgilerini tespit edebilmektedir.

g) İlgili firma ve kuruluşlardan gönderilen kimlik ve adres bilgisi kontrol edilerek şüpheli şahıs tespit edilir.

h) Savcılığın talimatı doğrultusunda başka suç ve suç delillerinin elde edilebilmesi amacıyla şüpheli şahsın ikametine veya işyerine arama, el koyma ayrıca arama sonucu elde edilecek olan bilgisayar ve diğer dijital materyaller üzerinde CMK'nın 134. maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde, hard disklerinde arama, inceleme, izin talebinde bulunulur.

i) Arama esnasında tespit edilen dijital materyallerin imajlarının alınarak incelenmesinde kullanılmak üzere ilgili Cumhuriyet Savcılığı'ndan el konulan materyallerin %30 fazlası hard disk fazlası talebinde bulunulur.

j) Tespit edilen dijital materyaller üst yazı ile içeriğinde inceleme izni bulunan mahkeme kararı ve soruşturma evrakının bir örneği ile Siber Suçlarla Mücadele Şube Müdürlüğü'ne elden teslim edilir.

k) İnceleme sonucunda hazırlanan rapor ve dijital materyaller soruşturma birimince teslim alınır.

l) Rapor ve diğer deliller doğrultusunda suçla iligli şüpheli şahsın konu hakkında ayrıntılı ifadesi alınır.

Coşkun Sapkın'ın müstehcen görüntüleri basın yayın yoluyla yayınlaması;

a) Müşteki savcılık makamından havaleli dilekçe ile birlikte İlçe Emniyet Müdürlüğüne gelir.

b) Müştekinin dilekçedeki/savcılık ifadesindeki bilgiler yeterli değilse ayrıntılı ifadesi alınır.

c) Site ile ilgili internet üzerinden **www.tib.gov.tr** adresinden whois sorgusu yapılır.

d) Site hakkında web tespit raporu tanzim edilir.

e) İnternet sitesine giriş yapılan bilgisayarın IP numaraları sitenin hosting firmasından (yer sağlayıcı) talep edilir.

f) Şüpheli IP adresi servis sağlayıcıdan (Türk Telekom'dan) sorulur. Son 3 aylık uygulamada; TİB'in yetkilendirmiş olduğu Emniyet Müdürlüğü'nde bulunan birim sayesinde şüphelinin IP adresini tespit için servis sağlayıcılara yazı yazma gereksinimi sona ermiştir. Söz konusu birim, çok daha kısa bir süre içinde şüphelinin IP bilgilerini tespit edebilmektedir.

g) İlgili firma ve kuruluşlardan gönderilen kimlik ve adres bilgisi kontrol edilerek şüpheli şahıs tespit edilir.

h) Savcılığın talimatı doğrultusunda başka suç ve suç delillerinin elde edilebilmesi amacıyla şüpheli şahsın ikametine veya işyerine arama, el koyma ayrıca arama sonucu elde edilecek olan bilgisayar ve diğer dijital materyaller üzerinde CMK'nın 134. Maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde, hard disklerinde arama, inceleme, izin talebinde bulunulur.

i) Arama esnasında tespit edilen dijital materyallerin imajlarının alınarak incelenmesinde kullanılmak üzere ilgili Cumhuriyet Savcılığı'ndan el konulan materyallerin %30 fazlası hard disk fazlası talebinde bulunulur.

j) Tespit edilen dijital materyaller üst yazı ile içeriğinde inceleme izni bulunan mahkeme kararı ve soruşturma evrakının bir örneği ile Siber Suçlarla Mücadele Şube Müdürlüğü'ne elden teslim edilir.

k) İnceleme sonucunda hazırlanan rapor ve dijital materyaller soruşturma birimince teslim alınır.

l) Rapor ve diğer deliller doğrultusunda suçla ilgili şüpheli şahsın konu hakkında ayrıntılı ifadesi alınır.

Hasan Münasebetsiz tarafından işlenildiği iddia edilen müstehcen görüntü içeren ürünlerin üretiminde çocukların kullandığı içeriklerin basın ve yayın yoluyla kullanıma sunulması " nun soruşturması;

a) Müşteki savcılık makamından havaleli dilekçe ile birlikte ilçe emniyet müdürlüğüne gelir.

b) Müştekinin dilekçedeki/savcılık ifadesindeki bilgiler yeterli değilse ayrıntılı ifadesi alınır.

c) Site ile ilgili internet üzerinden **www.tib.gov.tr** adresinden whois sorgusu yapılır.

d) Bahsi geçen porno sitesi hakkında web tespit raporu tanzim edilir.

e) Ayrıca bu siteyle ilgili çocuk pornosu yayınlamasından ve çocuk pornosunun 5651 sayılı Kanun kapsamında erişimin engellenmesi kararı çıkartılması için katalog

suçlardan olduğundan, erişimin engellenmesi kararı çıkarmak amacıyla soruşturma başlatılabilir.

f) Whois sorgusu neticesinde sitenin yabancı menşeli olması durumunda, yabancı ülke ile Türkiye arasında adlî yardımlaşmaya ilişkin sözleşme olup olmadığına bakılarak, site hesabına giriş yapılan bilgisayarın IP numaraları adlî yardımlaşma yoluyla ilgili ülkeden istenmelidir.

g) IP numarasının elde edilebilmesi tespit edilen kimlik bilgilerinin başkaca toplanan deliller ile sabit olması durumunda kimlik ve adres bilgileri kontrol edilerek şüpheli tespit edilir.

h) Savcılığın talimatı doğrultusunda başka suç ve suç delillerinin elde edilebilmesi amacıyla şüpheli şahsın ikametine veya işyerine arama, el koyma ayrıca arama sonucu elde edilecek olan bilgisayar ve diğer dijital materyaller üzerinde CMK'nın 134. Maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde, hard disklerinde arama, inceleme, izin talebinde bulunulur.

i) Arama esnasında tespit edilen dijital materyallerin imajlarının alınarak incelenmesinde kullanılmak üzere ilgili Cumhuriyet Savcılığı'ndan el konulan materyallerin %30 fazlası hard disk fazlası talebinde bulunulur.

j) Tespit edilen dijital materyaller üst yazı ile içeriğinde inceleme izni bulunan mahkeme kararı ve soruşturma evrakının bir örneği ile Siber Suçlarla Mücadele Şube Müdürlüğü'ne elden teslim edilir.

k) İnceleme sonucunda hazırlanan rapor ve dijital materyaller soruşturma birimince teslim alınır.

l) Rapor ve diğer deliller doğrultusunda suçla iligli şüpheli şahsın konu hakkında ayrıntılı ifadesi alınır.

VAKA ANALİZİ 5

Akif Kibar, inşaat alanında danışmanlık veren İnşa A.Ş. nde pazarlama müdürü olarak çalışmaktadır. İnşa A.Ş. şirketi, sektörüyle ilgili projelerin yayınlandığı, kullanıcıların projelere teklif verdiği, bu alandaki aktörlerin bir araya geldiği bir web projesi üzerinde çalışmaktadır.

İnşa A.Ş.nin en büyük rakiplerinden olan Yapım A.Ş.nin buna benzer bir web projesi faaliyettedir. Bahsi geçen rakip firmanın projesi olan "yapiyapi.com"; ücretli üyelikle hizmet veren bir web sitesidir. Akif Kibar, kendi projelerine katkıda bulunacağını düşündüğü için, bu siteyi incelemek istemektedir. Bir gün şirket kataloglarının hazırlanması için uzun süredir çalışmakta oldukları Oz Ozalitçisi'ne gittiğinde, orada bulunan bilgisayarlardan bir tanesinin ekranında rakip firmanın web sitesinin açık olduğunu fark etmiştir. Bunun üzerine Oz Ozalitçi'de çalışan Berrin Beyaz'dan üyelik bilgilerini kullanarak siteyi incelemek için izin istemiş; ancak Berrin Beyaz böyle bir yetkisi olmadığını söyleyerek teklifi reddetmiştir. Berrin Beyaz'ın oradan uzaklaştığı sırada, Oz Ozalitçisi'nin kullanıcı adını öğrenmiş, ofise döndükten sonra kullanıcı adı ile birçok defa şifre denemiş ve bir şifrenin doğru olduğunu fark etmiştir.

Akif Kibar sonrasında, şirket bilgisayarından bu bilgileri kullanarak "yapiyapi.com"a erişim sağlamıştır. Bu sayede şirketlerinin web projeleri için birçok fikir elde etmiş ve bunları kullanmıştır. Bunun sonucunda İnşa A.Ş. şirketinin web projesi kısa sürede tamamlanmış ve **www.insainsaatdanismanlik.com** alan adıyla hizmet vermeye başlamıştır.

Rakip firmanın sitesine aynı anda iki kişinin girebilmesi mümkün olmadığı için, Oz Ozalitçi yetkilileri bir başkası tarafından sisteme girildiğini fark etmişlerdir. Bunun üzerine savcılığa suç duyurusunda bulunulmuş ve savcının olayı soruşturduğu sırada dinlediği Berrin Beyaz, Akif Kibar'ın kendisinden üyelik bilgilerini istediğini; ancak vermediğini, kendisi oradan uzaklaştığı sırada bilgileri masa üstündeki defterden almış olabileceğini söyledi.

SORULAR

1. Akif Kibar rakip firmanın bahsi geçen projesinin yer aldığı alan adının altında kullanıcı adı ve şifreyi ele geçirmede hangi teknik yöntem kullanmıştır, açıklayınız.

2. Olaydaki suç tipini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.

3. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir? Açıklayınız.

4. 5651 sayılı Kanun'a göre "yapiyapi.com" firmasının hukukî statüsü nedir, açıklayınız.

5. yapiyapi.com yabancı menşeli bir firma olsaydı, log kayıtlarının temin edilmesi için hangi usulün izlenmesi gerektiğini açıklayınız.

6. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

CEVAPLAR

1. Akif Kibar rakip firmanın bahsi geçen projesinin yer aldığı alan adının altında kullanıcı adı ve şifreyi ele geçirmede hangi teknik yöntem kullanmıştır, açıklayınız.

Akif Kibar'ın uygulamış olduğu teknik yöntem şifre kırma saldırısıdır. Bir bilgisayar sisteminden iletilen ya da bir bilgisayarda saklanan verilerin şifresini kurtarma veya öğrenme işlemine şifre kırma denir. Bu konuya genel yaklaşım, bütün tahminleri tek tek denemektir. Şifre kırma işlemi, bilgisayar şifresini unutan insanlar için yardımcı olabilir. Şifre kırma işlemi ayrıca dijital dünyada gizli verilere erişim olanağı da sağlar.

Bir şifreyi kırmak için gereken zaman şifrenin bir uzunluğuna ve karmaşıklığına göre değişebilir, bu ölçüm aslında şifrenin entropy'sinden sağlanır, yani şifre içinde sadece harf ve sayılar değil ^%&/();? gibi karakterler de kullanılırsa şifrenin karmaşıklığı artar. "Brute-force cracking" ismi verilen Kaba-Kuvvet Saldırıları ile bir şifrenin olabilecek bütün şifre olasılıkları tahmin edilir ve denenir. Bu denemelerden birisi mutlaka gerçek şifreyi yakalar. En çok kullanılan şifre kırma yöntemleri -mesela Sözlük atağı (dictionary attacks), Pattern Checking, Kelime listesi yerine koyma yöntemi... v.b. yöntemler – deneme sayısını azaltır ve genelde Brute-Force ataktan önce kullanılır.

2. Olaydaki suç tipini tespit ediniz, kime/kimlere karşı hangi suç işlenmiştir, açıklayınız.

a) Akif Kibar, yetkisiz olarak hukuka aykırı bir şekilde rakip firma Yapım A.Ş.'nin websitesine girme ve orada kalmaya devam etme suretiyle TCK m 243'te düzenlenen "Bilişim Sistemine Girme Suçu"nu işlemiştir.

b) Şüphelinin dolandırıcılık fiili gerçekleştirmek için para talep ettiği iddia edilen hesap numarasının ait olduğu kişinin bilgilerine ihtiyaç vardır. Bu bilgiler Banka'dan talep edilir.

3. Olayda delil elde etme yöntemlerinden hangisi/hangileri kullanılmalıdır, kullanılacak olan yöntem/yöntemler ile hangi deliller elde edilir, açıklayınız.

Şüphelinin tespit edilmesinden sonra başkaca bir suretle delil elde edilmesinin mümkün olmaması nedeniyle, CMK madde 134'e göre Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına hâkim tarafından karar verilir. Delillerin sağlıklı biçimde toplanabilmesi, olay yerine yapılan ilk müdahâlenin ne kadar sağlıklı olduğuna bağlıdır. Adlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde edilirken bilgisayardaki verilerin mevcut hâli ile yedeği alınmalı, bilgisayar iade edilmeli ve yapılacak arama işlemi bu yedek üzerinde yapılmalıdır. Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifre çözümünün yapılması ve gerekli kopyaların alınması hâlinde, el konulan cihazlar gecikme olmaksızın

iade edilir. Şüphelinin bilgisayarında bizzat bulundurulması suç olan kredi kartı şifreleri, çocuk pornografisi vb. mevcut ise yedeklerin verilmemesi gerekmektedir. Çıkartılacak yedekten şüpheliye veya vekiline örnek verilmesi bu kişilerin isteğine bırakılmıştır. Ancak şüpheliye örnek isteyip istemediği sorulup bu husus kayıt altına alınmalıdır. Delil toplamadaki başarı oranı, bilişim suçlarıyla mücadelenin önemli bir göstergesidir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz saptanması ve zarar görmeden toplanması, ilk olay yeri müdehalesinin düzgün yapılmasıyla mümkündür. Adlî bilişim uzmanının, delil kaybını mümkün olan en alt düzeye indirmek için gerekli olan bilgiye ve deneyime sahip olması çok önemlidir. Delil elde etme çalışması sırasında, olay yerinde varsa (örneğin güvenliği sağlayan) konu hakkında bilgi ve tecrübesi olmayan kişilerin aygıt ve sisteme müdehaleleri kesinlikle engellenmelidir. Kriminal inceleme yürütülürken elektronik deliller de toplanmalı, bunun için öncelikle delillerin nerede ve hangi formatta olduğu, nasıl depolandığı tespit edilmelidir. Sonrasında, ortamda bulunan elektronik donanımların çalışma biçimleri ve birbirlerine bağlılıkları tespit edilerek buna göre hareket edilir. Örneğin, olay yerinde kapalı konumda bulunan bir bilgisayar varsa kesinlikle açılmamalı; açık bir bilgisayar ise kesinlikle doğrudan kapatılmamalıdır. Bilgisayarın açılması hâlinde işletim sistemi çalışacak ve bilgisayar verileri işlemeye başlayacaktır. Bunun sonucu ise, verilerin üzerine yeniden veri yazılması ve potansiyel delillerin kaybı olabilecektir. Bilgisayar açık ise kesinlikle hiçbir program çalıştırılmamalı, hatta bilgisayar kapatılmamalıdır. Herhangi bir programın çalışması, bir potansiyel delilin kaybı anlamına gelebilir. Bilgisayar çalışıyor konumda fakat ekranı siyah ise, ekranın açık olup olmadığı kontrol edilmeli, sonrasında fare (mouse) oynatılarak görüntünün gelmesi sağlanmalıdır. Çalışmakta olan bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesi, doğal olarak o anda ve olay yerinde mümkün olamayacaktır. Bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gereklidir. Kapatılması dahi veri kaybına yol açabilecek bir donanımın götürülmesi durumunda öncelikle bilgisayar üzerinde bulunan ve çalışma konumundan çıkınca yok olabilecek tüm bulgular tespit edilerek belirlenmeli, kesinlikle ekran görüntüsü fotoğraflanmalı, çalışan programlar varsa not edilmeli ve bilgisayar kapatılmayarak, arkadaki güç kablosu çekilmelidir. Bunun yapılması belki birtakım verilerin kaybına yol açabilecekse de, delillerin bütünlüğünün bozulmasının önüne geçecektir. Delillerin tümünün kaybındansa, az miktar verinin kaybı daha tercih edilir bir durumdur. Kaldı ki bilgisayardaki tüm delillere adlî bilişim uzmanlarınca ve laboratuar ortamında çeşitli analizler yapılmaksızın ulaşılması çok olası bir durum değildir. Delil araştırma amaçlı olarak yapılacak incelemeler, donanımlar üzerinde değil, alınan kopyaları üzerinde yapılmalıdır. Bu, donanımlar içerisindeki verilerin kaybını önleyecektir. Aygıtlardaki verilerin sağlıklı kopyalarının alınması çok önemlidir. Adlî bilişimde yapılan birebir kopyalama işlemine imaj (birebir kopya) denilmektedir. Bu kopyalama, sistemdeki tüm verilerin, özel yazılımlar veya donanımlar kullanmak suretiyle ve bit-bit başka bir ortamda bir örneğinin (imajının / birebir kopyasının) oluşturulması suretiyle yapılır. Adlî imajın önemi, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşma olanağını vermesidir. Sistemden imajı alınmış verilerin tümünün gözle görünür hâle getirilmesinden sonra analiz aşamasına geçilecektir. Adlî bilişimin son safhası raporlama ve yetkili makama sunma safhasıdır. Raporlama safhası, hukukî bir değerlendirmeyi içermektedir. Değerlendirmeyi adlî bilişim uzmanı değil, kolluk yapar. Adlî bilişim uzman(lar)ının inceleme aşamasından geçmiş verilerden hangilerinin delil olabileceği, o suç için kullanılabilir nitelikte olduğu soruşturmada görevli kolluk tarafından değerlendirilir ve adlî makamlara sunulur.

4. 5651 sayılı Kanun'a göre "yapiyapi.com" firmasının hukukî statüsü nedir? Açıklayınız.

Yapiyapi.com'da sektöre ilişkin haberler site sahibi tarafından yayınlandığı için İçerik sağlayıcı; 5651 sayılı Yasa'nın 2. maddesinin 1. fıkrasının f bendinde, "internet ortamında kullanıcılara her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir." şeklinde düzenlenmiştir. İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

5. www.yapiyapi.com yabancı menşeli bir firma olsaydı, log kayıtlarının temin edilmesi için hangi usulün izlenmesi gerektiğini açıklayınız.

Bilişim suçlarının en önemli özelliklerinden birini de bu suçların genellikle sınır aşan bir biçimde işlenmesi ve buna bağlı olarak uluslararası bir boyutunun olmasıdır. Dolayısıyla günümüzde bilişim suçlarıyla ilgili olarak uluslararası kuruluşlar ve çalışmalar olduğu gibi, çok ciddi hukuksal düzenlemeler de bulunmaktadır. Nitekim ulusal hukuklarda konuyla ilgili olarak yapılan düzenlemelerin çoğu ya uluslararası düzenlemelerden alınmış ya da bunlara uyumlu hâle getirilmiştir. Özellikle Avrupa Siber Suç Sözleşmesinin yürürlüğe girmesinden sonra taraf ülkeler için durum tam bu şekildedir. Türkiye açısından uluslararası adlî yardımlaşmaya ilişkin çok taraflı ve iki taraflı anlaşmalar bulunmaktadır. Türkiye'nin Amerika Birleşik Devletler ile arasında ceza istinabe konusunda ikili antlaşmalar bulunmaktadır. Uluslararası istinabeye ilişkin sözleşmelerden biri de Avrupa Siber Suçlar Sözleşmesi'dir. Siber Suçlar Avrupa Sözleşmesi'ni; Amerika Birleşik Devletleri, İngiltere, Fransa, Almanya, Japonya'nın da dâhil olduğu 10 devlet imzalamış ve ulusal parlamentosunda onaylayarak yürürlüğe koymuştur. Türkiye'nin de arasında olduğu 37 ülke Sözleşmeyi imzalamış ancak henüz parlamentosundan geçirmemiştir. Sözleşme 2012 yılı Aralık ayında onay için TBMM'ye gönderilmiş, Meclis Dışişleri Komisyonunda kabul edilerek Genel Kurula sevk edilmiştir. Hâlen Genel Kurul gündemine alınması beklenmektedir. Siber suçlarda şüpheliye ulaşmak için en yaygın şekilde kullanılan yöntem şuça konu işlem yapılırken kullanılan IP numarası tespit edilerek, IP numarasının tahsis edildiği internet abonesini belirlemektir. Bu tür suçlarla ilgili olarak yapılan uluslararası adlî yardımlaşma taleplerinin büyük çoğunluğu da IP numarası veya trafik verisinin ilgili firmadan temin edilmesi talebini içermektedir.

6. Şüphelinin tespiti için gerekli olan soruşturma aşamalarının neler olduğunu tespit ediniz.

a) Müşteki savcılık makamından havaleli dilekçe ile birlikte İlçe Emniyet Müdürlüğüne gelir.

b) Müştekinin dilekçedeki/savcılık ifadesindeki bilgiler yeterli değilse ayrıntılı ifadesi alınır.

c) Müştekinin dilekçede gösterdiği tanık Bayan B dinlenir.

d) Yetkisiz erişilen site ile ilgili internet üzerinden **www.tib.gov.tr**

adresinden whois sorgusu yapılır.

e) Yetkisiz erişilen site hakkında web tespit raporu tanzim edilir.

f) Söz konusu sitenin yer sağlayıcısı olan firmadan, yetkisiz erişimin meydana geldiği tarihlerdeki IP adresleri sorulur.

g) Yer sağlayıcısından elde edilecek bilgilerden yola çıkılarak söz konusu alışverişleri yapan internet abonesinin tespiti için Telekom Müdürlüğü veya diğer servis sağlayıcılardan gerekli bilgi ve belgelerin elde edilir.

h) İlgili firma ve kuruluşlardan gönderilen kimlik ve adres bilgisi kontrol edilerek ve başkaca delillerin de aynı kişiyi göstermesi sonucunda şüpheli şahıs tespit edilir.

i) Savcılığın talimatı doğrultusunda başka suç ve suç delillerinin elde edilebilmesi amacıyla şüpheli şahsın ikametine veya işyerine arama, el koyma ayrıca arama sonucu elde edilecek olan bilgisayar ve diğer dijital materyaller üzerinde CMK'nın 134. Maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde, hard disklerinde arama, inceleme, izin talebinde bulunulur.

j) Arama esnasında tespit edilen dijital materyallerin imajlarının alınarak incelenmesinde kullanılmak üzere ilgili Cumhuriyet Savcılığı'ndan el konulan materyallerin %30 fazlası hard disk fazlası talebinde bulunulur.

k) Tespit edilen dijital materyaller üst yazı ile içeriğinde inceleme izni bulunan mahkeme kararı ve soruşturma evrakının bir örneği ile Siber Suçlarla Mücadele Şube Müdürlüğü'ne elden teslim edilir.

l) İnceleme sonucunda hazırlanan rapor ve dijital materyaller soruşturma birimince teslim alınır.

m) Rapor ve diğer deliller doğrultusunda suçla iligli şüpheli şahsın konu hakkında ayrıntılı ifadesi alınır.