YARGITAY KARARLARI IŞIĞINDA DOĞRUDAN BİLİŞİM SUÇLARI[1025],[1026] (TCK. 243 ve 244)

Nevzat ÖZSOY

BİRİNCİ BÖLÜM

I- GİRİŞ

Bilişim suçları, Yargıtay Kararlarında kabul edildiği üzere;

- Doğrudan bilişim suçları (gerçek bilişim suçları); TCK. m. 243, 244, 245, 245/A ve 246. maddelerinde yer alan suçlar,

- Dolayısıyla bilişim suçları (bilişim bağlantılı suçlar); TCK. m. 112, 113, 125, 132, 133, 134, 135, 136, 138, 142/2-e, 158/1-f, 213, 218, 226 ve 228. maddelerinde yer alan suçlar şeklinde bir tasnife tabi tutulmaktadır.[1027]

Bilişim suçları Türk Ceza Kanun'un 10. Bölümde 243, 244 ve 245. Maddelerinde düzenlenmiştir, bu bölümde yer alan 243.maddenin 1.fıkrasında bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme veya 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, 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 hali 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,

1025 Nevzat ÖZSOY Yargıtay 8. Ceza Dairesi Üyesi
1026 ORCİD: orcid.org/0000-0001-8749-6333
1027 Yargıtay Ceza Daireleri uygulamasında sıklıkla rastlanan bozma sebepleri, Yargıtay Cumhuriyet Başsavcılığı, Ankara 2018 s. 829

kendisi veya bir başkası yararına sağladığı haksız çıkarın, bir başka suçu oluşturmaması halinde bu fıkra uyarınca cezalandırılması öngörülmüş, 245. Maddesinde ise banka ve kredi kartlarının kötüye kullanılması suç olarak düzenlenmiştir.

Ancak TCK.nun 245. Maddesinin bilişim suçları kategorisi içerisinde düzenlenmesi yerinde değildir. Bu suçun Yasa'nın 2.Kitabının 2.Kısmının 10.Bölümünde yer alan "Malvarlığına Karşı Suçlar" arasında düzenlenmesinin daha doğru olacağı düşünülmektedir. Bu çalışmada sadece TCKnın 243 ve 244. maddelerinde düzenlenen doğrudan bilişim suçları inceleme konusu yapılmıştır.

07.04.2006 tarihinde yürürlüğe giren 24.03.2016 tarihli 6698 sayılı Kanunun 30. maddesi ile birinci fıkradaki "ve" ibaresi "veya" olarak değiştirilmiş, gerekçe ile metin arasındaki çelişki giderilerek eylem seçimlik hale getirilmiştir. Ayrıca aynı Kanun ile 243. maddeye 4. fıkra eklenmiş, yeni bir suç düzenlemesi yapılmıştır. Ancak bu düzenlemede "bilişim sistemine girme" sözkonusu olmadığından ilk üç fıkradan farklı bir düzenleme yapılmıştır. [1028]

II- KAVRAM ve TANIM

1.Bilişim; bilginin saklanması ve iletilmesini konu alan akademik ve mesleki disiplin olarak tanımlanabilir. Bilişim, insanların teknik, ekonomik, sosyal, kültürel, hukuksal ve benzeri alanlarda sahip oldukları verinin saklanması, saklanan bu verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve yüksek hızlı veri, ses veya görüntü taşıyan iletişim araçları ile aktarılmasıdır. Böylece bilişim, hem verilerin işlenmesini hem de bu işlem sonuçlarının aktarılmasını yani veri iletişimini de içeren bir kavramdır. O halde, veri – işlem ve veri – iletişim unsurlarını taşıyan araçların bütününe bilişim sistemi denilmektedir.

2.Bilişim suçu; bilişim suçunu "verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alnında işlenen, bir bilgisayar ya da ağına yönelik olarak ya da onları kullanarak icra edilen her türlü yasadışı haksız eylem olarak tarif etmek mümkündür."

"Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenilen suçlardır." "Bilişim Teknolojileri kullanılarak işlenen tüm suçlar "Bilişim Suçlarını" oluşturur."

"Bilgisayar suçu (computer crime): Bir bilgisayar ya da bilgisayar ağına yönelik ya da onları kullanarak (bilgisayar teknolojisi bilgilerinden yararlanılarak) gerçekleştirilen yasa dışı eylem."

1028 Gül, Ahmet, Doğrudan Dolaylı Bilişim Suçları, Seçkin, Ankara, 2019 s. 56,57

"Siber suçlar (cyber crimes): Herhangi bir suçun elektronik ortam içerisinde işlenebilme imkanı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil genel olarak hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçları siber suçlar olarak tanımlayabiliriz. Siber suç bilgisayar ve ağ sistemleri yoluyla bilgisayar veya ağ sistemleri içerisinde ya da bilgisayar tarafından suç olarak yaratılmış fiillerin siber ortamda işlenmesi ve daha önce suç olarak yaratılmamış bu ortamın karakteristiğe has bir takım ihmallerin bir bütünüdür."

Tanımlarda da görüldüğü gibi bilişim suçlarının net olarak çizgileri çizilmemiştir çünkü gelişen teknolojiyle birlikte bilişim suçları da değişmektedir. Bu nedenle "bilişim suçları", "bilgisayar suçları", "internet suçları", "siber suç", "ileri teknoloji suçu", "dijital suçlar", "sanal suç" gibi kavramların tek bir tanımının yapılmaması bir eksiklik olarak değerlendirilmemelidir. Ancak biz bu kavramların hepsini genel olarak "bilişim suçu" olarak adlandırabiliriz. Günümüzde bilişim suçlarına "**internet suçları"** ismi verilmektedir.

3.Bilişim sistemi; verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağını veren manyetik sistemlerdir.Bu tanımın, sadece "veri – işlemi" esas alması, "veri – iletişimine" yer vermemesi bakımından eksik olduğu belirtilmektedir.[1029] Bilişim sisteminin, bilgileri otomatik olarak işleme tabi tutması ve manyetik olması dışında ki en önemli özelliği genel amaçlı kullanım özelliğidir. Yani belli bir işin yapılmasına özgülenip başka bir fonksiyon eda edemeyen bir sistem bilişim sistemi değildir. Mesela; otomatik çamaşır makineleri, elektronik uzaktan kumandalı TV, programlanabilen buzdolabı, genel amaçlı işlem yapamadıklarından yani yüklenen değişik programlara göre başka nitelikli işlemleri yapamadıklarından, bilişim sistemi olarak kabul edilmeyecektir.[1030]Bilgisayar, çevre birimleri (bir bilgisayarın çalışması için zorunlu olmayan ancak kullanımını kolaylaştıran hoparlör, CD ROM, 297ery, klavye, kulaklık, yazıcı vb), iletişim altyapısı (elektronik haberleşme, internet, intranet gibi) ve programlardan oluşan veri işleme saklama ve iletmeye yönelik sistemi ifade eder.

4.Bilişim alanı; bilgileri depo ettikten sonra bunları otomatik olarak işleme tabi tutan sistemlerden oluşan alan olarak tanımlanabilir.[1031]

1029 Prof. Dr. Mehmet Emin Artuk, Prof. Dr. Ahmet Gökçen, Doç. Dr. Caner Yenidünya, Türk Ceza Kanunu Şerhi, Özel Hükümler, C. 5, s.4643, Ankara 2009

1030 Levent Kurt, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınevi, s.141, Ankara 2005

1031 Yrd. Doç. Dr. R. Yılmaz YAZICIOĞLU, Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı, s.2, 21-22 Mayıs 2001, İzmir Uluslararası İnternet Hukuku Sempozyumunda sunulan tebliğ.

5.Bilgisayar; belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, yürüteceği 298ery298f298 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).

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

7.Elektronik Veri; elektronik, 298ery298 veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları ifade eder (bkz. 5070 Sk'nun 3/a mad.)

8.IP (Internet Protocol) Adresi; belirli bir ağa bağlı cihazların birbirini tanımak, birbirleri ile iletişim kurmak ve birbirlerine 298ery yollamak için kullandıkları, internet protokolü standartlarına 298ery 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.

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.

9.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.

10.Mac (Media Access Control) Adresi; Ethernet ağında sistemler birbirlerinden sahip oldukları MAC adresi ile ayırt edilirler. Ethernet, wi-fi, ery299f299gibi ortamlarda ağ donanımını tanımlamaya yarayan, bir bilgisayarın ery299f299 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.

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)

11.Bilgisayar Kütüğü; bilgisayarın ve bilgisayarda yer alan dosyaların, geçirdiği safahatlara dair kayıtların tutulduğu verileri ifade eder.

12.Sunucu Kütüğü; bir sunucudaki bütün değişikliklerin kayıt altına alındığı kütük dosyasını ifade eder. Kütüklerde bilgisayar ağına erişim, dosyalarda yapılan değişikler, 299ery f indirme ve yükleme gibi kayıtlar tutulur.

13.Bilgisayar Programı; bilgisayara bir işi yaptırmak için verilen komutlar bütününe bilgisayar ery299f299denir. Bilgisayar 299ery299f299 bir programlama dili kullanılarak yazılır. Program çalıştırıldığında bilgisayar ilgili komutları okuyarak programda kendisine ery299f edilen işi yapar

14.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.

15.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. Adli 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.

16.Bilişim Ağı (Network), Internet, Internet Ortamı, Intranet, Bulut Bilişim (Cloud Computing):

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

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

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

İntranet; 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.

17.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.

18.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.

19.Yer Sağlayıcı, Içerik 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.

20.Trafik Bilgisi (Log Kayıtları); internet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, 301ery, yararlanılan hizmetin türü, aktarılan 301ery 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 bilgileri ifade eder.

III. BİLİŞİM SUÇLARINDA SORUŞTURMA, GÖREVLİ VE YETKİLİ MAHKEME

A- SORUŞTURMA

5237 sayılı Türk Ceza Kanunu'nun 243 ve 244. maddelerinde düzenlenen bilişim suçları şikâyete bağlı suçlardan değildir. Bu suçlar nedeniyle Cumhuriyet savcıları resen soruşturma başlatabilir.

5271 sayılı Ceza Muhakemesi Kanunu'nun 160. maddesi uyarınca Cumhuriyet savcısı TCK. nun 243 ve 244. maddelerinde belirtilen bilişim suçlarından her hangi birisinin işlendiğini öğrendiğinde, bir şikâyet beklemeksizin gerekli araştırma ve soruşturmayı yaparak yeterli delil elde ettiği takdirde CMK. nun 170. maddesi gereğince kamu davasını açacaktır.

B- GÖREVLİ MAHKEME

5237 sayılı TCK. nun da 243 ve 244. maddelerinde düzenlenen bilişim suçlarında hangi mahkemenin görevli olduğuna dair Kanun metninde bir düzenlemeye yer verilmemiştir. Bu nedenle görevli mahkeme 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 10. 11. ve 12. Maddelerine

göre belirlenecektir. Bu bağlamda TCK. Nun 243 ve 244 . maddelerinde düzenlenen suçlar bakımından görevli mahkeme asliye ceza mahkemeleridir.

C- YETKİLİ MAHKEME

Bilişim suçları konusunda yer bakımından yetki konusunda suçun niteliği ve işleniş şekilleri nedeniyle çok fazla sorun yaşanmaktadır.

Bilişim suçlarında yer yönünden yetki konusunda özel bir düzenleme bulunmadığından yer yönünden yetkili mahkeme Ceza Muhakemesi Kanunu'nun 12. maddesinin 1 ve 2. fıkralarına göre belirlenecektir.

Ceza Muhakemesi Kanunu'nun 12. Maddesindeki düzenlemeye göre davaya bakmak yetkisi suçun işlendiği yer mahkemesine aittir. Eğer eylem teşebbüs aşamasında kalmış ise son icra hareketinin yapıldığı, kesintisiz suçlarda da kesintinin yapıldığı yer mahkemesi yetkili olacaktır. Seçimlik hareketli fiiller ile işlenebilen bilişim suçları teşebbüse de müsait suçlardır. Dolayısıyla yer yönünden yetkili mahkemenin tayininde CMK.nun 12. maddenin 1-2. fıkralarının işlerliği farklı olabilecektir.

TCK. nun 243. Maddesinde düzenlenen bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme ve orada kalma suçlarında yetkili genel kural gereği suçun işlendiği yer mahkemesi, **sistemin tamamına ya da bir kısmına hukuka aykırı olarak girilen yer yani** gerçekleşen fiilin icra edildiği yer mahkemesi olan asliye ceza mahkemesi olacaktır.

Türk Ceza Kanunu'nun 243/1. madde ve fıkrasında belirtilen girme veya kalma eylemleri seçimlik hareketlidir. Sisteme hukuka aykırı olarak girmek veya kalmak suçu oluşumu için yeterlidir. Bu nedenle **CMK. nun 12/2 maddesi gereği eylemin sona erdiği yer mahkemesi yetkili olacaktır.**

TCK. nun 244. Maddesinde düzenlenen suçlar birden fazla seçimlik hareketi içerdiğinden, engelleme, bozma, veri yerleştirme, veri yok etme veya verileri değiştirme fiillerinin işlendiği yer mahkemesi yer yönünden yetkili mahkemedir.

TCK. nun 243 ve 244. maddelerinde düzenlenen eylemlerin teşebbüs aşamasında kalması halinde ise yine genel kural gereği son icra hareketinin yapıldığı yer mahkemesi yer yönünden yetkili mahkeme olacaktır.

Bu suçların uluslar arası alanda işlenmesi halinde ise yer yönünden yetki sorunu Türk Ceza Kanunu'nun 8. Maddesi çerçevesinde çözümlenecektir. Burada da yetki konusunda hem "**suçun işlendiği yer**" hem de "**sonucun gerçekleştiği yer**" esas alınarak genel bir düzenleme yapılmıştır.

Artuk – Gökçen – Yenidünya'ya göre; bilişim sistemine fiziksel temas ile girilmesi halinde eylem nerede yapılmışsa suç orada işlenmiştir. Buna karşılık bilişim sistemine ağ üzerinden erişilmiş ise bu takdirde suçun araç bilişim sisteminin bulunduğu yerde mi, yoksa hedef bilişim sisteminin bulunduğu yerde mi işlendiği tartışılabilir. Hareketin parçaları veya hareket ile netice arasında siyasi ve coğrafi sınır bulunan bu tür suçlara mesafe suçu denilmektedir. Kanımızca burada bilişim suçlarının özellikleri dikkate alınarak suç, hareket, hareketin kısımları ve neticenin gerçekleştirildiği her yerde işlenmiş sayılmalıdır. Böylece bilişim suçlarının cezasız kalması önlenmiş olacaktır. Nitekim TCK.nun 8. maddesinde; "fiilin kısmen veya tamamen Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır" denilerek sınır aşan mesafe suçları basımından ortaya çıkabilecek tartışmalara son vermiştir. Şu halde, gerek içeriden dışarıya (failin ağa bağlandığı bilişim sisteminin Türkiye'de, hedef bilişim sisteminin yurt dışında olması), gerekse dışarıdan içeriye (failin ağa bağlandığı bilişim sisteminin yurt dışında, hedef bilişim sisteminin Türkiye'de olması) mesafe suçları Türkiye'de işlenmiş sayılır[1032]

İKİNCİ BÖLÜM

I.5237 SAYILI TÜRK CEZA KANUNU'NUN 243. MADDESİ

A.Hukuka Aykırı Olarak Bilişim Sistemine Girme Ve Orada Kalma

Madde 243 -(*1*) *Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren* ***veya*** *orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir. (24.03.2016 tarihli ve 6698 sayılı Kanunun 30. maddesi ile yapılan değişiklikle birinci fıkrada yer alan "ve" ibaresi "veya" olarak değiştirilmiştir)*

(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

"(4)Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır" *(24.03.2016 tarihli ve 6698 sayılı Kanunun 30. maddesi ile maddeye 4. fıkra eklenmiştir)*

Madde Gerekçesi

1032 Artuk, Gökçen, Yenidünya, age s. 4633-4634

Bilişim sistemlerine karşı suçların düzenlendiği bölümde yer alan bu maddede bilişim sistemine girme fiili suç olarak tanımlanmıştır.

Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.

Maddenin birinci fıkrasında bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiili suç hâline getirilmiştir. Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir.

İkinci fıkraya göre, birinci fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, bu suç açısından daha az ceza ile cezalandırılmayı gerektirmektedir.

Üçüncü fıkrada, bu suçun neticesi sebebiyle ağırlaşmış hâli düzenlenmiştir. Birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.

Sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır.

Bilişim sistemine girmekten kasıt sistemin donanımsal bölümüne girmek değildir. Burada girmekle ifade edilen sisteme erişimdir.*"izinsiz erişim"* Avrupa komisyonu tarafından bilgisayar sistemleri bir bölümüne ya da tümüne yapılan izinsiz erişimleri tanımlamak için kullanılmıştır.[1033]

5651 sayılı Kanuna dayanarak çıkarılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usül ve Esaslar Hakkında Yönetmelik'in tanımları açıklayan 3/1-e maddesinde ve 01.11.2007 tarihinde yayınlanan İnternet Toplu Kullanım Sağlayıcılar Hakkındaki Yönetmelik'in tanımları belirleyen 3/1-c maddesinde "erişim" kavramı kullanılmış ve erişim her iki düzenlemede de "herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılmasını ifade eder." şeklinde tanımlanmıştır.[1034]

Yargıtay 8. Ceza dairesinin yerleşik kararlarında belirtildiği gibi "Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden

1033 Erdoğan, Dr. Yavuz, Türk Ceza Kanununda bilişim sistemini engelleme bozma verileri yok etme değiştirme suçu, Doktora tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011, s.110
1034 Erdoğan, s.111

virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Bu suç, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi, bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır.

E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikâyeti üzerine öncelikle erişimi engellenen adresin şikâyetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adresin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (internet Protokolu) numarası sorulmalıdır. Microsoft Corporation'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde e-mail adresine giriş yapılıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli ve loglar üzerinde inceleme yapılmalıdır[1035]

1.Korunan Hukuki Yarar

Bu suçla korunan hukuki yarar karma bir nitelik taşımakla birlikte asıl olan bilişim sisteminin güvenliğidir. Ancak bu suç bilişim sisteminin güvenliği yanında, verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı ya da kişilerin ya da kurumların ihtiyaç duyduğu güvenlik duygusu gibi kişilerin farklı türden çıkarlarını da koruma altına almaktadır. Ancak tüm bunların üstünde ve bunları kapsayacak şekilde yer alan hukuksal değer bilişim sisteminin güvenliğidir.[1036]

Madde ile sistemdeki veriler ele geçirilmeden verilere hukuka aykırı olarak erişim suç haline getirilmiştir. Sisteme erişimin sağlanmasından sonra kişisel verilerin hukuka aykırı olarak

1035 Bakınız. Y.8.CD. 11.10.2017 gün, 2016/12839, 2017/11114, 26.03.2009 gün 18190/3058, 07.05.2014 gün 2013/10402, 2014/11836

1036 Doç. Dr. Murat Volkan Dülger, bilişim suçları ve internet iletişim hukuku, Ankara 2015, sh. 348 gül, G, ag, s. 57

ele geçirilmesi durumunda ayrıca TCK. nun 136. maddesinde düzenlenen "verileri hukuka aykırı olarak verme veya ele geçirme" suçu, verilerin sistemden tamamen kaldırılarak ele geçirilmesi durumunda ise TCK. nun 244/2. maddesinde düzenlenen suç gündeme gelecektir.[1037]

2.Suçun Unsurları

a.Fail

Bu suçun faili herkes olabilir. Özgü bir suç değildir. Çünkü madde metninde suçu işleyecek kişi açısından herhangi bir özellik belirtilmemiştir.

Fail kendisi için ya da başkaları için (bilişim sistemine girebilir) suçu işleyebilir.

TCK.nın 246. maddesindeki "bu bölümde yer alan suçların (243, 244, 245) işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur." düzenlemesi karşısında fail bir tüzel kişinin temsilcisi ya da onun yararına suç işlerse TCK.nun 20. maddesi gereğince tüzel kişiye ceza verilmez, ancak aynı kanunun 60. maddesindeki güvenlik tedbirleri uygulanabilir.

Failin belirlenmesi suçun sübutuna ilişkin bir husus olup failin doğru belirlenmesi, iyi bir soruşturma gerektirir. 8. Ceza Dairesinin bir çok kararında eksik araştırmadan bozma kararı verilirken ilamlarda soruşturmanın ne şekilde yapılması gerektiği de anlatılmaktadır. (Y. 8. C.D. 11.10.2017 gün, 2016/12839, 2017/11114)

b.Mağdur

Mağdur, belirli bir suçla zarara veya tehlikeye uğratılan hak veya çıkarın, suçla korunan hukuksal değerin sahibi olan kişidir. Bu suçun mağduru açısından da Yasa metninde bir özellik gösterilmemektedir, herkes bu suçun mağduru olabilir. Bilişim sisteminin güvenliğinin ihlal edilmesiyle çıkarı zarara uğratılan kişi suçun mağduru olmaktadır. Suçun mağdurunun ancak gerçek kişiler olabileceğini kabul eden yazarlar yönünden tüzel kişiler bu suçun mağduru değil suçtan zarar görenidir. [1038] Bununla birlikte bir kişiye ait bilişim sistemine izinsiz olarak girildikten sonra, bir başka kişinin gizli kalması gereken kişisel bilgilerinin elde edilmesi (veri nakli

1037 CD.11.02.2014gün, 2012/32093-2014/2779 "...suça konu .....@hotmail.com ve .....@yahoo.com elektronik posta adresleri hesaplarının oluşturulduğu sırada elektronik posta hizmeti veren şirketlere beyan edilen kimlik bilgilerinin ilgili yerlerden tespit edilerek, sanığın eyleminin TCK.nun 136/1. madde ve fıkrasında düzenlenen "kişisel verileri hukuka aykırı olarak verme veya ele geçirme" suçunu oluşturup oluşturmayacağı tartışılmadan yazılı şekilde hüküm kurulması, Yasaya aykırı"

1038 Dülger, age, sh. 359, Yaşar, Osman/Gökçen, Hasan Tahsin/Artuç, Mustafa yorumlu uygulamalı Türk Ceza Kanunu, cilt IV, Adalet Yayınları, Ankara 2010, sh. 6739

olmaksızın) halinde bu kişisel bilgilerin sahibi de TCK.nın 135, 136. maddelerinde tanımlanan suçlar yönünden suçun mağduru olacaklardır.[1039]

8. Ceza Dairesi uygulamasında gerek gerçek kişi gerekse tüzel kişiler suçun mağduru olarak tanımlanmaktadır.[1040]

c. Suçun Konusu

Birinci fıkrada düzenlenen suçun hukuki konusu içine girilen ve kalınan bilişim sisteminin kendisidir. Üçüncü fıkrada düzenlenen suç açısından bilişim sisteminde yer alan verilerdir. İkinci fıkrada düzenlenen cezayı hafifletici hal için ise suçun konusu bedeli karşılığı yararlanılabilen verilerdir.

Burada dikkat edilmesi gereken husus; TCK.nun 243/3. madde ve fıkrasındaki hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.

d. Eylem

Suçun oluşabilmesi için "***hukuka aykırı olarak girme ve orada kalmaya devam etme***" eyleminin birlikte gerçekleştirilmesi gerekmekte iken TCK'nun 243. maddesinin 1. fıkrasında 24.03.2016 tarihli ve 6698 sayılı Kanunun 30. maddesiyle yapılan değişiklikle birinci fıkrada yer alan "*ve*" ibaresinin madde gerekçesine uygun olarak "*veya*" şeklinde değiştirilmesi üzerine suç seçimlik hareketli hale gelmiştir.

Daha önce Yargıtay uygulamalarında girme aynı zamanda kalmayı da içerir, suçun oluşması için bir zarar meydana gelmesine ya da bir menfaat sağlanmasına gerek yoktur. Zaten bu soyut tehlike suçudur. Bu nedenle bir milisaniye bile kalınsa suç oluşur şeklinde bir yaklaşım vardı. Başka bir anlatımla failin sisteme girdiğini fark etmesiyle derhal çıkmaması durumunda suçun işlendiği kabul edilmekteydi.

Yeni düzenleme ile eylem seçimlik hareketli hale geldiğine göre "*orada kalmaya devam etme*" eyleminin oluşabilmesi için belirli bir süre aranacak mı?

Bilişim sistemine hukuka aykırı olarak girme veya orada kalma eylemlerinin gerçekleşmesi için sistemde ne kadar süreyle kalınacağı konusunda kanunda bir açıklık yoktur. Ancak suçun soyut tehlike suçu olması ve sisteme hukuka aykırı olarak girme veya kalma sonucunda bir zararın doğması ya da bir yarar sağlanması gerekli olmadığından, sisteme hukuka aykırı olarak girilmesi veya sisteme girildikten sonra bir milisaniye dahi kalınması halinde dahi suç oluşacaktır. Sistemde

1039 Erdoğan, age, s.116
1040 8. CD. 19.03.2018, 2494-2967 18.01.2018, 22781-560

kalma süresinin herhangi bir işlem yapmaya elverişli olması gibi bir zorunluluk ta yoktur. Çünkü bu sırf hareket suçudur.

Eylem olarak gösterilen "girme" ve "sistemde kalma" kavramlarından anlaşılması gerekenin "erişim" olarak tarif edilen eylem olduğundan Yargıtay kararlarında da bu kavram kullanılmaktadır. (bknz. Ekli kararlar 3,4,5,7) Ayrıca fail bilişim sistemine hukuka uygun olarak girip izni bittikten sonra hukuka aykırı olarak kalmaya devam etmesi durumunda da TCK.nun 243/1. maddesindeki suç oluşacaktır.

e. Suçun (Cezayı Hafifletici) Nitelikli Hali

TCK 243. maddesinin 2. fıkrasında, hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma eylemlerinin, "bedeli karşılığı yararlanılabilen sistemler" hakkında işlenmesi cezayı hafifletici bir neden olarak öngörülmüştür.[1041] Buna göre, maddenin 1. fıkrasında tanımlanan fiillerin, bedeli karşılığı yararlanılan sistemler hakkında işlenmesi indirim nedenini oluşturmaktadır.

Gerek madde metninde gerekse de gerekçede bedeli karşılığında yararlanılan sistemin ne olduğu konusunda bir açıklamaya yer verilmemiştir. Ancak bedeli karşılığında yararlanılan sistemlere internet üzerinden ücret karşılığı hizmet veren web siteleri, oyun siteleri vb. örnek olarak gösterilebilir[1042]. Bunların hepsinde kişiler belli bir bedel karşılığı bir bilişim sistemine girip sistemin kendisinden ya da sağladığı hizmetlerden yararlanmaktadır. Kanunda geçen bu kavramdan anlaşılması gereken TCK.nın 163. maddesinde yazılı ve karşılıksız yararlanma suçunun konusunu oluşturan otomatlar değildir.[1043]

f.Suçun Neticesi Sebebiyle Ağırlaşmış Hali

TCK.nun 243. maddesinin 1. fıkrasındaki suçun kasten işlenmesi sonucunda; istenmediği halde (yani sonuç yönünden kastı bulunmaksızın) bilişim sisteminin içerdiği verilerin yok olması ya da değişmesi hali 3. fıkrada suçun neticesi sebebiyle ağırlaşmış hali olarak düzenlenmiştir. TCK.nun 23. maddesi de gözetildiğinde burada sonuç yönünden sanığın en azından taksirinin bulunması aranmaktadır. Fıkradaki sonuçlar sadece "verinin yok olması" ve "verinin değişmesi" ile sınırlı tutulmuştur. Elbette bu netice sebebiyle ağırlaşma hali, diğer iki fıkra için de

1041 1-Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması,
2-Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince arttırılması gerektiğinin gözetilmemesi, Y. 8. CD. 08.01.2014. 2012/33044-2014/236.
1042 Bozma sebepleri, s.833
1043 Gül, age, s.64

geçerlidir.[1044] 8. Ceza Dairesinin uygulamasında TCK.nun 61/4 maddesi uyarınca önce TCK.nun 243/3. maddesindeki nitelikli halden temel ceza belirlenip daha sonra aynı maddenin 2. fıkrasına göre indirim yapılacaktır.

3.Suçun Manevi Unsuru

TCK.nun 243/1. maddesinde düzenlenen bilişim sistemine girme veya sistemde kalmaya devam etme suçu kasten işlenebilen bir suçtur. Failin bilişim sistemine izinsiz/yetkisiz girdiğini bilmesi yeterlidir. Taksirle işlenebileceğine dair bir düzenleme bulunmadığı için suçun taksirle işlenmesi mümkün değildir. Ancak, bilişim sistemine girme ve sistemde kalmaya devam etme eylemi sırasında sistemin içerdiği veriler yok olur veya değişirse bu durumda aynı Yasanın 243/3. maddesindeki düzenleme akla gelecektir. Yasa maddesinin bu fıkrasındaki eylemin gerçekleşmesi için kast aranmaz. Failin hukuka aykırı olarak sisteme girmesi ve kalması sırasında istemeyerek sisteme ve verilere zarar verilmesi durumunda bu hüküm uygulanacaktır. Örneğin sanığın bir bilişim sistemine hukuka aykırı olarak girmesi veya orada kalmaya devam etmesi sırasında istemeyerek sistemdeki verilere zarar vermesi gibi.

Bu nedenle maddenin 3. fıkrasında düzenlenen eylemde kast yoktur, kastın aşılması söz konusu olacaktır. Yani failin sisteme zarar verme amacı yoktur. Eğer fail sisteme hukuka aykırı ya da uygun olarak girdikten sonra isteyerek bir zarar verirse bu durumda TCK. nun 244/2. maddesi gündeme gelecektir.

Bu fıkranın uygulanabilmesi için failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir. Yoksa fail, verileri bilerek ve isteyerek yok ederse TCK'nın 244/2. maddesindeki suç oluşacaktır.

4.Hukuka Aykırılık Unsuru

TCK'nun 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalmaya devam etme suçu açısından söz konusu olabilecek hukuka uygunluk nedenleri, TCK. nun 24/1. maddesinde düzenlenen "kanunun hükmünü yerine getirme" ve TCK. nun 26/3. maddesinde düzenlenen "ilgilinin rızası"dır.[1045] Rıza ancak hak sahibi olan kimse tarafından verilebilir[1046]. Örneğin bir soruşturma gereği bilişim sistemine girilmesi durumunda eylem suç teşkil etmeyecektir.

1044 Aksi görüş için bkz. Dülger, age, s. 360
1045 Dülger, age. s.390.391, Yaşar/Gökçen/Artuç, age s.6746
1046 Dülger, age, s.391

Rıza, hukuka aykırılığı ortadan kaldırır. Ancak, rızanın suçun işlendiği sırada var olması gerekir. Fiil sonrasındaki şikâyetçi olmama, suçu ortadan kaldırmaz.

5.Suçun Özel Görünüş Şekilleri

a.Teşebbüs

Birinci fıkrada belirtilen bilişim sistemine girme ve sistemde kalma hareketlerinin yapılmasıyla suç tamamlanmış olacaktır. Bu fıkrada düzenlenen suç için ayrıca bir netice (zarar) aranmamıştır. Birinci fıkrada düzenlenen suça teşebbüs mümkündür. Şöyleki; sisteme girmek için gerekli icrai hareketlerin başlamasına rağmen girme veya kalma eyleminin gerçekleştirilememesi halihde teşebbüs hükümleri uygulanabilecektir. Zira sisteme girilmek istenirken internet bağlantısının kesilmesi, elektriğin kesilmesi veya şifreli bir sitem için şifrenin çözülememesi gibi durumlarda eylemin teşebbüs aşamasında kaldığından bahsetmek mümkün olacaktır.

6698 sayılı Yasa ile yapılan değişiklik öncesi ancak bilişim sistemine girildikten sonra sistemde kalma fiili temadi niteliğinden dolayı bu fiil yönünden suçun teşebbüse elverişli olmadığı ile sürülebilinir[1047] ise de söz konusu yasa ile "ve" ibaresi "veya" olarak değiştirildikten sonra bu suça teşebbüs imkansız hale gelmiştir. Bunun yanında TCK. nun 243/3. maddesinde düzenlenen suçun neticesi sebebiyle ağırlaşmış hali yönünden ise teşebbüs olanaklı değildir.

b. İştirak

Madde metninde özel bir iştirak hükmüne yer verilmemiştir. Bu nedenle suçlara iştirak açısından bir özellik söz konusu olmayıp TCK.nun 37., 38., 39. ve 40. maddelerindeki suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir. Bu suçlara iştirak her zaman mümkündür.

c. İçtima

Bu suçların zincirleme şekilde işlenmesi mümkündür. Bilişim sistemine hukuka aykırı olarak girme ve orada kalma eylemi içerisinde bir süreklilik mevcuttur. Kalma eyleminin devam etmesiyle eylem gerçekleşmiş olacaktır. Suç zorunlu olarak bir mütemadi suçtur. Ancak fail sisteme girdikten sonra çok uzun süre kalır ve kalmaya devam ederse ne olacaktır? Zincirleme suç hükümleri uygulanacak mı? Sorunu gündeme gelmektedir. İşte failin bilişim sisteminde kalmasıyla temadi gerçekleşmiş olacağından fail hakkında zincirleme suç hükümlerinin uygulanma olanağı yoktur. Bu durumda TCK. Nun 3. ve 61. maddeleri uyarınca Hâkim madde metninde öngörülen cezanın alt ve üst sınırlarına göre bir ceza tayin edebilecektir.

1047 Dülger, age.

TCK.nun 43. Maddesinde düzenlenen zincirleme suç hükümlerinin uygulanması failin aynı suç işleme kararıyla bir bilişim sistemine farklı zaman dilimlerinde girmesi ve sistemde kalmaya devam etmesi halinde mümkün olacaktır. Örneğin sanık bir bilişim sistemine kısa aralıklarla birden çok girip orada kalır ve çıkarsa bu durumda faile verilecek cezanın TCK.nın 43. maddesi uyarınca arttırılarak verilmesi gerekir. Ancak fail aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla sisteme giriyor ve orada kalmaya devam ediyorsa bu durumda failin aynı suç işleme kararıyla hareket ettiği söylenemeyecek ve her eylem için ayrı ceza verilip cezaların içtimaı kuralı uygulanacaktır. [1048]

Failin eyleminin hem suçun nitelikli halini, hem de neticesi sebebiyle ağırlaşmış halini ihlal etmesi durumunda, yani bedeli karşılığı hizmet veren bir bilişim sistemine yetkisiz girip veya orada kalmaya devam ederken taksirli bir haraketiyle sistemde yer alan bazı verilerin yok olmasına ya da değişmesine neden olursa Yargıtay 8. Ceza Dairesi (suçun TCK.nun 243/2. maddesindeki nitelikli halinin işlenmesi sonucunda 3. fıkradaki neticenin oluşması halinde) her iki fıkranın da uygulanmasına karar vermektedir. Yani 3. fıkraya göre belirlenecek cezadan 2. fıkraya göre indirim yapılacaktır.

Bilişim sistemine hukuka aykırı olarak girme ve orada kalma eylemi açısında öne çıkan en önemli sorunlardan birisi, bir bilişim sistemine girilerek TCK. nun 244. maddesindeki "sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçunun işlenmesi durumunda ayrıca TCK. nun 243/1. maddesi uyarınca da ceza tayin edilip edilmeyeceğidir. Ancak TCK. nun 244. maddesindeki eylem, TCK. nun 243/1. maddesinde tanımlanan eylemi de içerdiğinden TCK.nun 44. maddesi uyarınca yalnızca TCK.nun 244. maddesi uygulanacaktır. [1049] Ancak 244. maddedeki eylemlerin gerçekleşmesi için bilişim sistemine girmeye veya kalmaya mutlaka gerek yoktur.[1050]

Fail TCK.nın 244/2. maddesindeki seçimlik eylemlerden birini gerçekleştirmek kastıyla değil de sadece sisteme girip kalmak maksadıyla girmiş, ancak sonradan 244/2. maddede belirtilen hareketlerden birini (kasten) gerçekleştirmiş (örneğin: e-postalarına bakmak için girmiş ancak şifreyi değiştirmiş) ise bu durumda eklenen kast nedeniyle TCK.nın 244/2. maddesiyle cezalandırılacaktır. [1051]

1048 "sanığın tespit edilen IP ile suç tarihinde bir kez girdiği ve kaldığı anlaşılmasına rağmen hakkında zincirleme suç hükümleri uygulanarak fazla ceza tayini" 8. C.D. 17.05.2017, 2016/9971, 2017/5660 bkz, benzer; 8. C.D. 04.06.2014, 2014/3984-13848,
1049 (Aksi görüş için bkz, Dülger, age, s...)
1050 (Gül, age, s. 87)
1051 (Gül, age, s. 87, aksi görüş için Dülger, age, s. 406,407)

8. Ceza Dairesi katılana ait ...hotmail.com internet adresinin ve Facebook hesabının fail tarafından şifrelerinin kırılmak suretiyle girip sonra da şifreyi değiştirerek sahibine karşı bilişim sisteminin erişilmez kılındığı takdirde TCK.nın 244/2. aksi takdirde aynı Yasanın 243/1. maddesi kapsamındaki suçun oluşacağına karar vermiştir. [1052]

Ayrıca TCK.nın 244/1 ve 2. fıkralarındaki suçların fail tarafından ayrı ayrı ihlal edilmesi, iki suçun da ayrı ayrı işlenmesi de mümkündür.[1053]

6.Yaptırım

TCK. nun 243/1. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalma suçunu işleyen failler için *"bir yıla kadar hapis veya adli para cezası"* öngörülmüştür. Bu cezalar seçimlik olarak düzenlendiği için iki cezanın birlikte verilmesi mümkün değildir; fail hakkında gerekçesi gösterilerek ya hürriyeti bağlayıcı ceza ya da adli para cezasına karar verilecektir.

Adli para cezasının tercih edilmesi halinde ceza miktarı TCK.nun 52. maddesinde gösterilen miktara göre beş günden az ve yediyüzotuz günden fazla olmamak üzere belirlenecektir.Ancak 5237 sayılı TCK.nun 61/9. maddesinin yürürlüğe girdiği 19.12.2006 tarihinden önce işlenen suçlarda 5 gün, bu tarihten sonra işlenen suçlarda ise 30 gündür. Adli para cezasının üst sınırı da 19.12.2006 tarihinden önce işlenen suçlarda 730 iken, bu tarihten sonra işlenen suçlarda 365 gündür[1054].

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 adli para cezası verilemeyecektir.

B- VERİ NAKİLLERİNİ İZLEME (TCK. m. 243/4)

07.04.2016 tarihinde Resmi Gazetede yayımlanarak yürürlüğe giren 24.03.2016 tarihli ve 6698 sayılı Kanunun 30. maddesi ile maddeye eklenen 4. fıkraya göre "*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır*"

6698 sayılı Kişisel Verilerin Korunması Kanunun Adalet Alt Komisyonu'nda yapılan görüşmesi sonucu düzenlenen raporda "Sanal Ortamda İşler Suçlar Sözleşmesi'nin 3. maddesiyle

1052 (Y. 8. C.D. 18.11.2015, 2015/7531-24704)
1053 (Gül, age, s. 88)
1054 Yaşar/Gökçen/Artuç, age. s.6752

üye ülkeler yasa dışı araya girme eylemini cezalandırmaya davet edildiğinden 5237 sayılı Kanunun 243. maddesinde değişiklik öngörülmüştür. Böylece bilişim sistemlerinin bütününe veya bir kısmına hukuka aykırı olarak girmekle birlikte belirli bir süre kalmak da suçun unsuru olarak düzenlenmiş olmasına rağmen sözleşmeye uyum amacıyla sadece sisteme/sistemlere girmek fiili suç olarak düzenlenmektedir. Verilerin izelenmesi eylemi, bilişim sistemlerine herhangi bir müdahalede bulunmaksızın teknik araçlarla bilişim sistemleri arasındaki veri nakillerinin takip edilmesini ifade etmektedir. Bütün elektronik veri transferleri, bu çerçevede korunması amaçlanan veri transferinin gizliliği kapsamında kalmaktadır. Yasa dışı araya girme eylemleri, temelde bilişim sistemlerine girmeksizin işlenen fiillerdir. Bu doğrultuda sözleşmeye uyum amacıyla yine aynı maddenin 1. fıkrasının hüküm eklemek suretiyle, bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla izleyen kişinin 6 aydan 3 yıla kadar hapis cezası ile cezalandırılması öngörülmüştür.

Bu fıkra hükmüne göre fail sisteme girmeksizin bir bilişim siteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini teknik araçlarla hukuka aykırı olarak izlenmelidir.

Bu fiil yönünden de mağdur ve fail yönünden bir ayrım yapılmamış olup, mağdur veya fail herkes olabilir. Suçun, hukuka aykırılık, kusurluluk, özel görünüş şekilleri yönünden birinci fıkradakı fiil ile ilgili yapılan anlatımlar geçerlidir. Eylem ile bir yarar sağlanması öngörülmemiş, tehlike suçu olarak düzenlenmiştir. Suç, kasten işlenebilen bir suçtur. Suçun konusu bilişim sistemleri arasında ya da aynı bilişim sisteminde nakledilen verilerdir.

Bu fıkraya göre öncelikle;

1- Öncelikle bilişim sisteminin kendi içinde veya bilişim sistemleri arasındaki veri nakilleri suçun konusu olabilecektir.

2- Sisteme girmeksizin eylem gerçekleştirilmelidir.

3- Eylem teknik araçlarla izleme şeklinde gerçekleştirilmelidir.

4- İzleme hukuka aykırı olarak yapılmalıdır. Mahkeme kararı gibi hukuka uygunluk nedenleri söz konusu ise maddedeki suçtan söz edilemeyecektir.

Bu izleme ile başkalarına ait kişisel verilerin ele geçirilmesi ya da özel hayatın gizliliğinin ihlal edilmesi durumunda TCK.nın 134, 135 ve 136. maddelerinin uygulanması gündeme gelecektir[1055].

1055 Gül, age, s. 65, 66

C- SORUŞTURMA VE KOVUŞTURMADA DİKKAT EDİLMESİ GEREKEN HUSUSLAR

Öncelikle belirtmek gerekir ki bilişim teknolojisi ve üretilen zararlı yazılım ve teknikler paralelinde değişen hukuki normlar ve mevzuat ile uygulamaya konulan stratejilerin birbirileriyle uyum ve ahenk içerisinde olmaması tehditlerle mücadelede kaynakların israf edilmesine ve gerekli önlemlerin etkin ve verimli olarak alınmamasına neden olmaktadır[1056].

8. Ceza Dairesinin 11.10.2017 gün, 2016/12839, 2017/11114 sayılı ve bir çok kararında belirtildiği üzere; bilişim suçlarından deliller büyük oranda soruşturma aşamasında toplanabildiğinden ve bu deliller ışığında bir sonuca varıldığından kovuşturma aşamasında yeni bir delil-bilgi temin edilebilmesi genellikle çok zor ya da imkansızdır. Bu nedenle soruşturma aşamasında toplanamayan deliller nedeniyle yargılama aşaması genellikle "delil yetersizliğinden beraat kararları" ile sonuçlanmaktadır. Sanal ortamda işlenen bu suçların delillendirilmesi oldukça güç olduğundan en önemli ve güvenilir delil dijital materyaller üzerinde yapılacak inceleme ve failin eylemi kabul etmesidir. Sanığın ikrarı az rastlanan bir durum olduğundan suça konu sistem üzerinde yapılacak inceleme son derece önemlidir[1057].

1. Müştekinin Kontrolünde Olan Sisteme Girme İddiası

Müştekinin kurulu bulunan sisteme yönelik eylem gerçekleştirildiğini iddia etmesi durumunda; öncelikle bu sistemin server (ana sunucu bilgisayarı) üzerinde adli bilişim uzmanlarınca inceleme yapılması ve yetkisiz erişim olup olmadığı, olşumşsa sisteme düşen IP adresi, URL adresi tespit edilmeye çalışılmalıdır. Keza server üzerinde tüm bilgilerin saklandığı ve diğer bilgisayarlara oranla daha hızlı ve kapasitesi yüksek bilgisayarlardır. İnceleme sonucu sisteme yetkisiz erişim, IP ve URL adresi tespit edildiğinde ilgili servis sağlayıcısından bu adres kullanıcısı internet abonesinin tespitine çalışılacaktır.

CMK 234. maddesinde yazılı mağdurun hakları ve CMK 161. maddesinde yazılı cumhuriyet savcılarının yetkileri çerçevesinde bu incelemenin yapılabilmesi için herhangi bir şekilde el koyma ya da inceleme kararına gerek yoktur. Ancak incelemenin delil değeri için müşteki tarafından değil, görevlendirilmiş adli bilişim uzmanları ya da bilirkişiler tarafından yapılması gereklidir.

1056 Efe, Dr. Ahmet, Bilişim Hukuku ile Uluslararası Hukuk Kesişiminde Yeni Bir Paradigma: Siber Yönetişim, Türkiye Noterler Birliği Hukuk Dergisi, Ankara, 2017, yıl:4 sayı:2 s.157
1057 Gül, age, s. 70

Uygulamada bu inceleme işlemleri uzun süre (aylar, bazen yıllar) aldığından, bu süreçte ilgili kurum, şirket ya da kişiler sistemi kullanamamaları nedeniyle mağdur olacağından sisteme yeni program yükleyip (formatlayıp) kullanmaya devam etmekte, sistem üzerindeki deliller elde edilememektedir. Neticede iddia edilen bir eylem ve dillleri olup olmadığı, iddianın inandırıcılığı tespit edilemeyeceğinden kovuşturmaya yer olmadığına dair karar verilecektir. Bunu engellemek maksadıyla topyalama, imaj alma yöntemleri izlenebilir. Yaşanan gecikmeler, yeterli sayı ve bilgi düzeyinde adli bilişim uzmanlığının önemini göstermektedir.

İnceleme yapılması için gerekli dijital materyaller (bilgisayar, cep telefonu, tablet, el bilgisayarı, dijital kamera ve fotoğraf makinesi, hard disk, flash gibi) şüphelenilen failde ise şartlar oluşması durumunda CMK 134. maddesindce yazılı arama, kopyalama ve el koyma yollarına başvurulacak, bu konuda sul hceza hakimliğinden karar alınacaktır. İnceleme sonucunda, veri saklamaya yarayan hard disk ve kullanıcının seyir defterini gösteren log kayıtları üzerinde yapılan inceleme son derece önemlidir. Bilgisayarlar arasında veri akışı olup olmadığı ayrıntılı bir şeiklde belirlenmelidir.

Yetkisiz erişim sağlandığı iddia edilen sistem bir bankaya ait ise, ilgili bankadan bir yazı ile inceleme sonucu elde edilen tüm bilgiler istenebilir.

Sisteme erişim sırasında tespite düşen IP adres bilgileri, sisteme ne şekilde girildiği, bu sistemden başkasına yarar sağlanıp sağlanmadığı, bilgi temin edilip başka yerde kullanılıp kullanılmadığı, sisteme zarar verilip verilmediği, TCK.nun 243. maddesinde yazılı suçlar harcinide başka suçların ayrıca oluşup oluşmadığını tespit bakımından önemlidir. Tespit edilecek IP adresi kullanıcıları bilgileri hızlı bir şekilde internet servis sağlayıcılarından (Türk Telekom, Aevea, Turkcell, Vodafone vs.) temin edilmelidir[1058].

2. Müştekinin Kontrolü Dışındaki Sisteme Yetkisiz Erişim

Bu iddialar genellikle e-posta hesabına izinsiz (şifre kırılarak girilmesi) sosyal paylaşım sitesi (facebook, twitter, instagram gibi) şifresinin kırılıp girilmesi, bu hesaplar üzerinden üçüncü kişilerin dolandırılması, yazışmalar yapılması, resimlerin paylaşılması ve hesaptan temin edilecek resim ya da kişisel bilgilerle hesap açılması şeklinde olabilmektedir.

Bu durum genellikle TCK.nun 243. maddesi dışındaki (TCK. 244, 158/1-f, 134, 135, 136 maddelerindeki suçlar gibi) suçları gündeme getirmekte ise de; eylemin niteliği ve ne şekilde gerçekleştiğinin tespiti için aynı yöntemin izlenmesi gerekecektir.

1058 Gül, age, s. 70,71,72

E-posta hesabına izinsiz girilerek bu hesap ile bağlantılı sosyal paylaşım sitesine girme eylemini araştırırken e-posta adresine müşteki harici erişim sağlanıp sağlanmadığı, ilgili şirket (Microsoft Corporation gibi) temsilciliğinden sorularak erişim sağlayan IP adres bilgileri temin edilebilecektir. Ancak ülke içinde temsilciliği olmayan şurt dışı kaynaklı servis sağlayıcısı (www.gmail.com, www.yandex.com, googlenin e-posta hizmet servisi, yahoo.com gibi) söz konusu olduğunda IP adresi bilgilerinin tespiti için istinade yoluna başvurulacaktır. Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nün web sitesinde duyurduğu üzere, özelilkle şirket merkezi ABD olan gmail.com'dan bilgi temini oldukça zor şartlara bağlı olmakla beraber, yabancı bir ülkenin kontrolündeki şirket verileri olarak iletilebilecek bilgilerin güvenilirliği/delil değerinde ayrı bir tartışma konusudur.

Aynı şekilde facebook, twitter, instagram gibi Amerikan menşeli sosyal paylaşım sitelerinden sisteme erişim sağlayan IP adreslerinin temini birinci kısımda değinildiği gibi oldukça sıkı şartlara bağlanmıştır.

Sadece hesabım çalındı, kişisel bilgilerin, fotoğraflarım paylaşıldı, hakaret edildi, arkadaşlarım hesabım üzerinden dolandırıldı gibi iddialarla IP adresinin tespiti mümkün olmadığından, dolayısıyla iddiaların doğruluğu araştırılıp sonuçlandırılamayacağından, soruşturma yapma imkanı olmadığından müracaatlar sonuçsuz kalacaktır. Ancak insan ticareti, çocuk pornosu, uyuşturucu ticareti gibi tüm dünyada hassasiyet gösterilen suçlarda Türkiye temsilcilikleri aracılığıyla bilgi paylaşımı yapılmakta, hassas davranılmaktadır.

D-TCK. NUN 243. MADDESİ İLE İLGİLİ YARGITAY KARARLARI

1.Sanığın soruşturma aşamasında müdafii huzurunda alınan beyanında katılan şirketten ayrıldıktan sonra katılan şirkete ait bilgisayar programına girdiğini kabul etmesi ve değişik zamanlarda bu programa girdiğinin dosya içerisindeki belgelerden anlaşılmış olması karşısında, sanığın oluşan eylemi nedeniyle bilişim sistemine izinsiz girme suçundan TCK.nun 243, 43. maddeleri gereğince cezalandırılması yerine dosya içeriğiyle uyuşmayan gerekçelerle beraat kararı verilmesi, (Y.8.CD. 04.06.2014 gün, 2014/3984-2014/13848)

2."Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine

yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Bu suç, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi, bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır.

E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikayeti üzerine öncelikle erişimi engellenen adresin şikayetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adresin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (internet Protokolu) numarası sorulmalıdır. Microsft Corporation'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde e-mail adresine giriş yapılıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli ve loglar üzerinde inceleme yapılmalıdır.

Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şikayetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.

Şikayetçiye ait e-mail adresine veya ele geçirilen adresten başkalarına, görüntü, yazı veya ses kaydı gönderildiğinin iddia olunması halinde ise, bu husus/hususlar üzerinde durularak gerekli tespitler yapılıp örnekleri de alınarak dosya içine konulmalıdır.

Şikayetçi ve şüphelilerin bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak görüntü ve yazı gönderilerek ulaşılan adres sahipleri tanık olarak dinlenmelidir.

Somut olayda; katılana ait .....@hotmail.com internet adresine sanık tarafından şifresinin kırılması yoluyla MSN adresine girilerek kullanılamaz hale getirildiği iddiasıyla açılan davada, sanık E.A'ya ve başka kişilere ait IP numaraları ile katılanın E-Mail hesabına giriş yapıldığının tespit edildiği, bu haliyle eylemin TCK.nun 243/1. Maddesi kapsamındaki suçu

oluşturacağı, ancak katılanın girişinin 04.05.2010 tarihi itibariyle engellediğini iddia etmişse de buna ilişkin bir tespite rastlanmadığının anlaşılması karşısında; anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, katılan tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit olunmamıştır. Sanık tarafından giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığının ilgili internet sağlayıcısından sorulmadığı anlaşılmıştır.

Bu itibarla yukarıda açıklanan yöntem izlenerek eksiklikler yerine getirilip sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, (Y.8.CD. 07.05.2014 gün, 2013/10402- 2014/11836**)**

3-Sanığın katılan şirkette çalıştığı sırada kendisine görevi nedeniyle verilen internet şifresini, iş yerinden ayrıldıktan sonra hakkı bulunmadığı halde kullanmak suretiyle katılan şirkete ait bilişim sistemine girdiği ve orada kalmaya devam ettiğini iddia ve sanığında bu iddiayı doğrulayan katılan şirkete ait bilişim sistemine hükümsüz kalan şifresi ile girip, buradaki şirket çalışanlarına ait maillerin kendi kurduğu siteye yönlendirmesini yapabilecek kadar süre ile kaldığını savunması karşısında; yüklenen TCK'nun 243/1. maddesindeki suçun bir bilişim sistemine hukuka aykırı olarak girmek ve orada kalmaya devam etmek unsurlarının gerçekleştiğinin kabulü ile mahkumiyetine karar verilmesi yerine yazılı şekilde beraatine hüküm kurulması, Y. 11. CD. 19.03.2012. 2009/22385-2012/3683.

4-Sanığın, katılanın yetkilisi olduğu ..... Tekstil Şirketinin Türkiye Ekonomi Bankası Denizli şubesinde bulunan hesabına internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında sanığın eyleminin 5237 sayılı TCK.nun 243/1. maddesinde düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde (5237 sayılı TCK.nun 244/4, 35/2. maddeleri gereğince) hüküm tesisi, (Y.11.CD., 26.03.2009, 18190/3058)

5- "... şifre değiştirildiğine ilişkin deliller tespit edilip değiştirilmediğinin tespiti halinde sanığın sadece bilişim sistemine giriş yaptığı ve kalmaya devam ettiğinin belirlenmesi halinde eyleminin TCK.nın 244/2. maddesinde düzenlenen suçu değil aynı Kanunun 243/1. maddesi kapsamındaki suçu oluşturacağı..." (Y. 8. C.D. 13.04.2017 gün, 2016/8243, 2017/4158)

6- ...şikayetçinin adresine girişinin engellendiğine dair bir tespitin bulunmaması karşısında; şikayet tarihinden önce Facebook adresinin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı araştırılarak ve şifrenin değiştirilip değiştirilmediği, değiştirilmişse

hangi tarihte ve hangi IP numarasından sağlanan erişim sonucu değiştirildiği ilgili internet sağlayıcısından ve Facebook şirketinden sorulup erişilmez kılındığı takdirde TCK.nın 244/2 aksi taktirde aynı Yasanın 243/1. maddesi kapsamındaki suçu oluşturacağı... (Y. 8. C.D. 2015/11993, 2016/3544)

7- ...gelen yazı cevaplarında şikayetçinin girişinin ne şekilde engellendiğine ilişkin bir tespite rastlanmadığının anlaşılması ve tüm dosya kapsamında, sanığın eyleminin TCK.nın 243. maddesi kapsamında değerlendirilmesi gerekirken... (Y. 8. C.D. 17.01.2018 gün, 2017/23248, 2018/501)

8- ...şikayetçinin hesabına sanığın giriş yaptığının tespit edildiği ancak dosya içerisinde e-mail şifresinin değiştirilmesine dair bir tespitin bulunmaması karşısında, sanığın sadece giriş yaptığı ve kalmaya devam ettiği anlaşılmakla eyleminin TCK.nın 243/1. maddesi kapsamındaki suçu oluşturacağı gözetilmeden... (Y. 8. C.D. 07.02.2018 gün, 2017/25385, 2018/1217)

9- "Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Suçun, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır.

E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikayeti üzerine öncelikle erişimi engellenen adresin ve sanığa ait olduğu iddia olunan e-mail adresinin sanığa ve şikayetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adreslerin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (İnternet Protokolu) numarası sorulmalıdır. Microsoft Corporation'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde şikayetçinin e-mail adresine giriş yapıp yapmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler

itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli, aynı şekilde sanığa ait olduğu iddia olunan e-mail adresini kullanan IP numaraları saptanıp adres ve telefon bilgileri de istenmelidir.

Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şika- yetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.

Şikayetçi ve sanığın bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp ele geçirilen adresten bir başka adrese yazı veya görüntü gönderilmiş ise, bu olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak ulaşılan adres sahipleri varsa tanık olarak dinlenmelidir.

Somut olayda; sanığın, şikayetçinin kullandığı ".....@hotmail. com" e-posta adresi ile irtibatlı olan facebook adresine bilgisi ve rızası olmaksızın şifreyi değiştirerek erişilmez kıldığından bahisle açılan davada, yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan hüküm kurulmuştur. Sanığın suçlamayı kabul etmediği gibi hattına başkalarının girmiş olabileceği savunmasına ilişkin olmak üzere internet hattını sanık dışında başkalarının da kullanıp kullanmadığı ve kendisine ait olduğu belirtilen e-mail adresinin sanığa aidiyeti hususunda dosyada bir bilgiye rastlanmamıştır. Şikayetçinin 05.12.2012 tarihinden itibaren e-mail adresine giremediğini belirttiğinin anlaşılması karşısında, anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit edilmemiştir. Sanık tarafından suç tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulmadan hüküm kurulmuştur.

Bu itibarla; yukarıda açıklanan yöntem izlenmeden yapılan soruşturma ve kovuşturma sonucu aradan geçen sürede dikkate alındığında bu eksikliklerin yerine getirilmesi imkansız hale gelmiş olmakla tebliğnamedeki bozma düşüncesine iştirak edilmemiştir.(Y. 8. C.D. 11.10.2017 gün, 2016/12839 - 2017/11114)

10- ...arkadaşlıklarının bitmesi üzerine bilahare sanığın, katılanın kullandığı elektronik posta adersine rızası dışında birçok kez girdiği olayda, sanığın, bu şekildeki eyleminin TCK.nın 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturduğu ve mahkemenin hükmün gerekçesinde de eylem bu şekilde kabul edildiği halde, sanık hakkında bilişim sistemine girme suçu

yerine, TCK.nın 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan hüküm kurulmak suretiyle sanık hakkında fazla ceza tayini, (Y. 12. C.D. 13.01.2016 gün, 2015/15933, 2016/277)

11- Katılan Şirketin sahibi olduğu web sitesi, müşterilerine ilan yapmaya kul- lanıcılarına da bu ilanları görmelerine imkan sağlayan dolayısı ile bu ilanlar üzerinden de karşılıklı iletişim sağlanarak alışveriş imkanı yaratan hizmet kolunda faaliyet gösterdiği ve kendisine verilen ilanlardan oluşan internet sitesi bazında bir veri tabanına sahip oldu- ğu, sanığın da bu şirkete ait web sitesindeki veri tabanınındaki ilanlara erişip izinsiz olarak kendisine ait internet sitesine gönderip kullanarak üzerine atılı bilişim sistemindeki verileri başka yere göndermek ve kullanmak suçunu işlediğinden bahisle açılan davada;

Sanık kurduğu sitenin arama motoru görevi gördüğünü, yaptığı işlerin link vermek şeklinde olduğunu savunmuştur. Katılan ise link verilmesi dahi izne tabi olup olayda sanık şirketin sayfasını kopyalayıp kendi sayfasına almış, ancak silemediği için logonun o sayfada görülmekte olduğunu belirterek şikayetçi olmuştur.

Bilirkişi, örümcek olarak tabir edilen bu sistemin çeşitli internet sitelerinde belirli kelime aramaları yaparak verileri çekmekte ve bu konuda arama motoru görevi yapmakta olduğunu, sitede ilanların hangi sayfadan alındığı görünmekte ve o siteye link verilmekte olup ilgilenen kişi gerçek bilgiye kendi sitesinde ulaşabildiğini bunların içerisinde katılan şirketin web sayfasında bulunan ilanların da bulunduğunun tespit edildiğini belirtmiştir.

İnternette ilanla mal satışlarında, ilanlar belirlenen süre ücretsiz olup daha sonraki ilanlar ücretli yayınlanabildiği dikkate alındığında ve dosya içinde bilirkişi raporuna ekli sayfa görüntülerinde; ilanda katılan şirketin logosu da dahil olmak üzere örneğin satılık arabanın resmi, teknik özellikleri, bedeli ve satıcı bilgileri tümüyle yayınlanıp alıcının tekrar katılan şirkete ait siteye gitmesine gerek kalmadığı açıkça görülmekte olup bilirkişi raporunda bahsolunan" çeşitli internet sitelerinde belirli kelime aramaları yaparak verileri çekmekte bu konuda arama motoru görevi yapmak"tan farklı olduğu anlaşılmakla, dosyaya uygun düşmeyen bilirkişi raporuna dayanarak ve eylemin TCK.nun 244/2. maddesindeki suçu oluşturup mahkumiyetine karar verilmesi gerektiği gözetilmeden, yazılı şekilde beraatine karar verilmesi, (Y. 8. CD 2013/4675, 2014/12406)

12- Sanık ile şikayetçinin bir dönem duygusal beraberlik yaşadıkları, ayrıldıktan sonra şikayetçinin kullanmış olduğu posta adresine habersiz olarak şifresini kırarak girdiği, bazı fotoğraflarını söz konusu hesaptan aldığından bahisle açılan davada,sanığın "..... kullanıcılar en az

270 günde bir oturum açmak zorundadırlar ve bu oturum belirtilen bu zamanda açılmaz ise mail hesapları kalıcı olarak şirket tarafından iptal edilir. Şikayetçi de bu Amerikan şirketinin kurallarına uymamış ve hesabını kalıcı olarak kaybetmiştir. Ben 01.04.2013 tarihinde bu hesabı yasal yoldan/sıfırdan/şifre kırmadan ve bilakis yeni şifre belirleyerek oluşturdum ve daha sonra şikayetçinin ricası üzerine benim olan bu hesabı kendisine kendi rızam ile teslim ettim"şeklindeki savunması karşısında, suç tarihinden önceki dönemde, bu adresin faal olup olmadığı, ve suç tarihinde önce ve sonraki tarihlerde şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı ilgili yer sağlayıcısından sorulup, sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, (Y. 8. CD 2016/9188, 2017/5663)

13- Sanığın tespit edilen IP ile suç tarihinde bir kez girdiği ve kaldığı anlaşılmasına rağmen hakkında zincirleme suç hükümleri uygulanarak fazla ceza tayini, (Y. 8. CD 2016/9971, 2017/5660)

14- ...sanığın soruşturma aşamasında müdafii huzurunda alınan beyanında katılan şirketten ayrıldıtkan sonra katılan şirkete ait bilgisayar programına girdiğini kabul etmesi ve değişik zamanlarda bu programa girdiğinin dosya içerisindeki belgelerden anlaşılmış olması karşısında, sanığın oluşan eylemi nedeniyle bilişim sistemine izinsiz girme suçundan TCK.nın 243, 43. maddeleri gereğince cezalandırılması yerine dosya içeriğiyle uyuşmayan gerekçelerle beraat kararı verilmesi...(8. C.D. 04.06.2014, 2014/3984-13848)

15- Sanık hakkında katılan Mehmet KESİCİ'nin rızası olmaması nedeniyle TCK.nun 168. maddesinde düzenlenen etkin pişmanlık hükümleri uygulanmamış ise de; banka tarafından üretilmiş kredi kartının henüz sahibine teslim edilmeden kullanılması halinde suçun mağdurunun banka olacağı cihetle ve katılan Mehmet KESİCİ'nin 9.2.2011 tarihli talimatla alınan beyanında sanığın babasının zararın 500 TL'lik kısmını kendisine ödediğini beyan etmesi karşısında mağdur bankadan sanık hakkında etkin pişmanlık hükümlerinin uygulanmasına rızası bulunup bulunmadığı sorularak sonucuna göre TCK.nun 168. maddesinin uygulanıp uygulanmayacağına karar verilmesi gerektiği gözetilmeden yazılı şekilde hüküm kurulması, (8. CD. 18.01.2018, 22781-560)

ÜÇÜNCÜ BÖLÜM

I. 5237 SAYILI TÜRK CEZA KANUNU'N 244. MADDESİ

A. BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİN ENGELLENMESİ VEYA BOZULMASI, VERİLERİN YOK EDİLMESİ VEYA DEĞİŞTİRİLMESİ SUÇUN (TCK. 244)

Madde 244 -(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 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.

Madde Gerekçesi

Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkrada seçimlik hareketli bir suç meydana getirilmiştir.

İkinci fıkrada, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi hâlinde, verilecek cezanın artırılması öngörülmüştür.

Üçüncü fıkrada ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.

Madde metninden de açıkça anlaşıldığı gibi 1. fıkrasında bir bilişim sisteminin işleyişini engelleme veya bozma, ikinci fıkrasında ise bir bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme fiilleri suç olarak tanımlanmıştır.

Maddenin 3. fıkrasında ki da 1. ve 2. fıkrasındaki fiilerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek ceza yarı oranında artırılacağı belirtilerek ağırlaştırılmış hal düzenlenmiştir.

Maddenin 4. fıkrasında ise maddenin 1. ve 2. fıkrasında tanımlanan fiillerin işlenmesi sonucunda kişinin kendisine veya başkasına haksız bir yarar sağlaması hali düzenlenmiştir. Failin maddenin 1. ve 2. fıkrasında tanımlanan fiilleri işlenmesi sonucunda kendisine veya başkasına haksız bir yarar sağlaması durumunda ise fiil başka bir suçu oluşturmuyorsa fail hakkında maddenin 4. fıkrası uyarınca ceza tayin edilecektir.

Burada dikkat edilmesi gereken husus, her ne kadar gerekçede fiilin daha ağır bir cezayı gerektiren başka bir suç oluşturmaması halinde bu hükmün uygulanacağı belirtilmekte ise de, madde metninde başka bir suçu oluşturmaması halinde bu hükmün uygulanacağı belirtildiğinden kanunilik ilkesi gereğince eylemin başka bir suçu oluşturmaması halinde bu fıkra uyarınca ceza tayin edilecektir.

TCK'nun 244. maddesinin 4. fıkrasında düzenlenen suç tali norm niteliğindedir. Bu hükmün uygulanabilmesi için fiilin başka bir suçu oluşturmaması gerekmektedir. 244. maddenin 1. ve 2. fıkralarında belirtilen fiillerin gerçekleşmesi durumunda haksız bir yarar da elde edilmiş ise bu durumda eylemin dolandırıcılık, hırsızlık, güveni kötüye kullanma gibi başka bir suçu oluşturup oluşturmadığı araştırılmalıdır. Eğer eylem bu suçlardan birini oluşturuyorsa artık 244. maddenin 4. fıkrası uygulanmayacaktır. Eylem bu suçlardan birisinin tanımına uymuyorsa, o zaman 244. maddenin 4. fıkrası hükmü uygulanabilecektir. 244. maddenin 4. fıkrası ancak eylemin başka bir suçu oluşturmaması halinde uygulanabilecektir. Örneğin eylem hırsızlık suçunu oluşturuyorsa artık TCK'nın 244/4. maddesi ile hüküm kurulmayacak, sadece oluşan hırsızlık suçundan hüküm kurulacaktır.[1059]

TCK.nun 244/1 maddesiyle bilişim sisteminin işleyişinin engellenmesi ve bozulması yaptırım altına alınırken özel bir zarar verme fiili düzenlenmiş olmaktadır. Nitekim inceleme konusu fıkranın gerekçesinde "böylece sistemlere yöneltilen ızrar fiilleri özel bir suç haline getirilmiştir." denilmek suretiyle bu görüşün haklılığı vurgulanmıştır[1060].

1.Korunan Hukuki Yarar

244. maddenin 1. ve 2. fıkrasında düzenlenen suçlarda korunan hukuki yarar bilişim sisteminde yer alan veriler ve yazılımlardır. Bir başka deyişle hem bilişim sisteminin hem de bu sistem içerisinde yer alan verilerin veya diğer unsurların sağlam ve güvenli bir şekilde çalışabilirliği

1059 2.CD. 19.06.2014 gün, 2014/22676-2014/17536."Sanıkların, katılanın banka hesabına bilgisi dışında intemet yoluyla erişim sağlayarak, hesabındaki parasını sanık Şahin Tüncer'in hesabına havale etmeleri şeklinde gerçekleştiği kabul edilen eyleminin 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen hırsızlık suçunu oluşturduğu gözetilmeden, yazılı şekilde aynı Kanunun 244/4 maddesi uyarınca hüküm kurulması."

1060 Erdoğan, age s.138

korunmaktadır.(Karagülmez Ali, bilişim suçları ve soruşturma-kovuşturma evreleri, Ankara 2011, sh. 211) Yani sistemin donanımı bu suçun kapsamı içerisinde değildir. TCK.nun 244. maddesindeki bu düzenleme Avrupa Konseyi Siber Suç Sözleşmesi'nin 4. ve 5. maddelerine ilişkin açıklayıcı rapora paralel bir düzenlemedir. Avrupa Konseyi Siber Suç Sözleşmesi'nin 4. ve 5. maddelerine ilişkin açıklayıcı raporda, 4. maddede korunan hukuksal değerin, bilişim sisteminde 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.[1061]

Ancak 244. maddenin 4. fıkrasındaki suçun oluşması için failin hukuka aykırı bir yarar elde etmesi gerekmektedir; ancak bunun nasıl bir yarar olduğu konusu açıklanmamıştır. Yararın türü bakımından bir ayrım yapılmadığına göre fail tarafından elde edilen maddi ya da manevi yarar suçla korunan hukuksal değeri oluşturmaktadır.

Ayrıca verilerin başka yere gönderilmesi, haberleşmenin engellenmesi durumunda üçüncü kişilerin özel hayatına ve haberleşme hürriyetine de müdahale söz konusudur[1062].

Bilişim sisteminin işleyişini sağlayan herhangi bir soyut unsura, sistemin bir bütün olarak kendisinden beklenen fonksiyonu yerine getirmesine engel olabilecek şekilde müdahalede bulunmakla suç oluşur. Bu tür müdahaleler çeşitli şekillerde gerçekleştirilebilir. Örneğin; bilgisayara virüs bulaştırılması, yazılım sisteminin çökertilmesi, bilgisayarın şifresinin değiştirilmesi, çok sayıda elektronik posta gönderilmek suretiyle sistemin işlemez hale getirilmesi gibi hareketler bu suçu oluştururlar. Keza, yoğun elektromanyetik dalgalarla sistem merkezi üzerinde etkide bulunmak suretiyle de sistemin işleyişi engellenebilir. Kısaca, bilişim sisteminin soyut unsuruna, sistemin kendisinden beklenen işlevi yerine getirmemesini sağlamaya yönelik her türlü müdahale bu suçu oluşturacaktır[1063].

Bu düzenlemeye göre, bir bilişim sisteminin donanım olarak ifade edilen (merkezi işlem ünitesi, klavye vs.) maddi unsurlarına yönelik zarar verici davranışlar bu madde hükmüne göre değil, mala zarar verme suçuna ilişkin hükümler (TCK m.151) çerçevesinde cezalandırılabilecektir. Buna karşılık yazılım olarak ifade edilen (programlar bütünü) sistemin işleyişini engelleyici veya

1061 Dülger, age, s.413
1062 Erdoğan, s. 146
1063 Taşdemir, Kubilay, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara 2009, s. 37.

bozucu davranışlar maddenin birinci fıkrası hükmüne istinaden ceza yaptırımı altına alınmış olmaktadır[1064].

2.Suçun Unsurları

a.Fail

Bu suçun faili herkes olabilir. Özgü bir suç değildir. Çünkü 244. maddenin 1., 2. ve 4. fıkralarında düzenlenen suçları işleyecek kişi açısından herhangi bir özellik belirtilmemiştir. 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.

b.Mağdur

Mağdur, belirli bir suçla zarara veya tehlikeye uğratılan hak veya çıkarın, suçla korunan hukuksal değerin sahibi olan kişidir. Gerçek kişiler suçun mağduru olabilir, bazı yazarlara göre[1065] 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. Bu suçun mağduru açısından da Yasa metninde bir özellik gösterilmemektedir, herkes bu suçun mağduru olabilir. 244. maddenin 1., 2. 3 ve 4. fıkralarında belirtilen hareketlerden birinin gerçekleşmesi durumunda çıkarı zarara uğratılan, bilişim sistemi ve/veya veriler üzerinde tasarruf yetkisi olan herkes olabilecektir.

c.Suçların Hukuki Konusu

244. maddenin 1. fıkrasında düzenlenen suçun hukuki konusu "*bilişim sistemi*"dir. 2. fıkrada yer alan suçun hukuki konusu ise "*bilişim sisteminde yer alan veriler*"dir. Bu nedenle 244. maddenin 1. fıkrasında düzenlenen suçu, 2. fıkrada düzenlenen suçtan ayıran en önemli husus suçun konusudur.

Bunun yanında 244. maddenin 4. fıkrasında düzenlenen suçun konusu ise failin sağladığı *"hukuka aykırı yarar"* oluşturmaktadır. 8. Ceza Dairesininin kararlarına göre bu yarar ekonomik değeri olan mali bir yarar yanında sosyal ve yönetsel bir statü değişikliği sonucunu doğuran bir manevi yararın da suçun hukuki konusunu oluşturduğu kabul edilmektedir.

1064 Prof.Dr. İzzet Özgenç, Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), s.1003, Seçkin Yayınevi 2005
1065 Dülger, age. s.359 Yaşar/Gökçan/Artuç age. s.6739

d.Eylem

aa)244. Maddenin 1. Fıkrasında Eylem

244. maddenin 1 fıkrasında "bilişim sisteminin işleyişini engellemek" ve "bilişim sisteminin işleyişini bozmak" fiilleri tanımlanmıştır. Bu fıkrada düzenlenen suçun oluşabilmesi için, ortada işleyişi engellenen veya bozulan bir "bilişim sistemi" bulunmalıdır.

Maddenin 1. fıkrasında "engelleme" ve "bozma" gibi iki seçimlik hareket düzenlenmiştir. Suçun oluşması için bu iki seçimlik hareketten birisinin gerçekleşmesi yeterlidir. İkisinin birlikte gerçekleşmesi halinde de "*tek suç*" vardır. Seçimlik hareketlerin birlikte gerçekleşmesi halinde hakim TCK.nun 3 ve 61. maddeleri çerçevesinde temel cezayı tayin edecektir.

aaa) Bilişim Sisteminin İşleyişini Engellemek

Bu fıkrada tanımlanan hareket, sistemin düzgün işlemesinden elde edilecek her türlü faydanın engellenmesi ve sistemin işlevlerini yerine getirmesine engel olan hareketlerdir. Yasa koyucu burada kavramı çok geniş tutmuş ve nasıl olduğunu aramaksızın sistemin işleyişini bozmak dışında, sistemin işlemesini engelleyen her türlü eylemi buraya dahil etmek istemiştir. Bu hareketlerle sistemin düzenli çalışması engellenmekte ya da sistem çalışamaz hale getirilmektedir. Böylece sistemin veri işleme hızı, düzenli çalışma yetenekleri olumsuz şekilde etkilenmektedir. Yoksa sistem bozulmamakta, ancak sağlıklı da çalışamamaktadır[1066]. Örneğin; sistem devamlı e-mail (e-posta) ya da zararlı virüs gönderilmek suretiyle çalışamaz hale getirilmektedir. Engellenme sürekli veya geçici olabilir.[1067]

bbb) Bilişim Sisteminin İşleyişini Bozmak

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.[1068]

Bozmak eyleminin gerçekleştirilme yöntemi, suçun oluşması bakımından önemli değildir. Böylece sistem çökertilmekte, verileri ve işleyiş düzeni bozulmaktadır. *"Sözlükte "engellemek", bir şeyin gerçekleşmesini veya yapılmasını önlemek; "bozmak" ise bir şeyi kendisinden beklenen*

1066 8.CD. 24.06.2013 gün, 2012/32866-2013/18872. "Katılana ait hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturarak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suça sürüklenen çocuğun eyleminin TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması"
1067 Taşdemir, age.
1068 Dülger age sh, 419

işi yapamayacak duruma getirmek; bir yerin, bir şeyin düzenini karıştırmak, dokunmak ve zarar vermek anlamlarına gelmektedir. Bu tanımlardan da anlaşılacağı üzere bokmak, engelleme sonucunu da doğuran bir anlama sahiptir. Bir bilişim sisteminin işleyişini bozan bir müdahale, aynı zamanda onun işleyişini engellemiş de olur. Ancak bu durum her iki kavramın aynı anlama geldiğini göstermez. Çünkü engellemek, bozmak demek değildir ve bir bilişim sisteminin işleyişi bozulmadan da engellenebilir" şeklinde açıklamıştır[1069].

Bilişim sistemine yapılan müdahalelerle sistemin veri işleme fonksiyonunu yerine getirememesi halinde bilişim sisteminin engellenmesi; sistemin işlem yapabilmesini sağlayan unsurlarına yapılan müdahalerle fonksiyonunu tamamen veya kısmen yerine getiremeyecek duruma sokulması halinde ise bozulması söz konusudur[1070].

Bilişim sistemine zarar vermek kastıyla icra hareketlerine başlayan failin fiziki saldırıları sonunda bilgisayarın kırılması durumunda (örneğin; balta ile vurulup parçalanması gibi), aynı zamanda bilişim sisteminin de bozulacağı mutlaktır. Failin tek fiil ile Yasanın çeşitli maddelerini ihlâl etmesi halinde, TCK.nun 44. maddesi uyarınca en ağır cezayı gerektiren aynı Yasanın 244/1. maddesi uyarınca cezalandırılması gerekir.[1071]

bb) 244. Maddenin 2. Fıkrasındaki Eylem

aaa)Verileri Bozmak

Bilişim sisteminin işleyişinin engellenmesi için verilerin bozulması halinde 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, sadece bir kısım verileri kullanılamaz hale getirmeyi amaçlamaktadır. Yani bir uygulama yazılımını ya da depolanmış bazı bilgileri kullanılamaz hale getirmek istemektedir.

bbb) Verileri Yok Etmek

Bilişim sistemindeki verileri tamamen ortadan kaldırmak ve varlığına son vermektir. Bu anlamda yok etme, verilerin silinmesini de kapsamaktadır. Ancak bilişim sistemindeki verileri her zaman tamamen ortadan kaldırmak-yok etmek mümkün değildir. Verilerin yok edilmesindeki kasıt verinin, mağdurun tasarruf alanından çıkartılmış olması ve normal yollardan ulaşılmasının güçleştirilmesidir. Yok edilen veriye, mağdurun kendisinin veya bir uzmanın tekrar ulaşabilme

1069 Koca, Prof. Mahmut, Hukukumuzda TCK.nun 244. maddesi kapsamında bilişim sistemini engelleme, bozma verileri yok etme ve değiştirme suçu, bilişim hukuk konferansı, 9-10 Ekim 2008, Yargıtay Yayınları s.93
1070 Koca, age. s93
1071 Taşdemir, age.

imkânının varlığı suçun oluşmasını engellemeyecektir. Bu nedenle yok edilmek eyleminden kasıt somut anlamda yok etmek eylemini değil, bilişim alanında geçerli olan soyut anlamda mantıksal yok etmek eylemini kastetmektedir. Örneğin; bir dosyanın geri dönüşüm kutusuna atılması gibi, verinin sistemde tutulmakla birlikte, sırf yerinin değiştirilmesi niteliğindeki hareketler bu suçu oluşturmayacaktır [1072].

ccc) Verileri Değiştirmek

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 ya da bir sistem içerisindeki bilgilerin değiştirilmesi şeklinde de olabilecektir[1073]. Örneğin kullanıcının sisteme koyduğu şifrenin yerine bir başka şifrenin konulması, bir bilginin değiştirilmesi halinde bu durum söz konusu olacaktır.

ddd) Verileri Erişilmez Kılmak

Burada veriler tamamen yok edilmemekte ancak sahibinin ya da ilgilisinin istediği zaman verilere ulaşması engellenmektedir. Bu hareket neticesinde veri bütünlüğü korunmaktadır, veri yok edilmemiş ya da bozulmamıştır, ancak verilere ulaşım bir şekilde engellenmiştir ve veri üzerindeki hak sahibi kendi verilerine erişememektedir. Bu sonuç bir kişinin bilgisayarına ya da bilgisayardaki dosyasına virüs bulaştırmak, şifre koymak gibi çok çeşitli şekillerde sağlanabilir.

Yargıtay 15. C.D. sinin 15.11.2016 tarih 2016/3781-8608 sayılı kararında "...sanığın, müştekinin elektronik posta adresinin şifresini kırarak, hesaba giriş şifresini değiştirerek, erişimini engellemesi şeklinde gerçekleşen eyleminin TCK.nın 244/2. maddesi kapsamında kaldığını..." kabul etmiştir.

eee) Bilişim Sistemine Veri Yerleştirmek

Bilişim sistemine veri yerleştirmek hareketiyle, maliki ya da ilgilisinden izin alınmaksızın çeşitli verilerin sisteme kaydedilmesi, yüklenilmesi ya da eklenilmesi kast edilmektedir. Bu yerleştirme hareketi "harici bellek" ya da "USB" gibi veri taşıma aracını sürücü donanıma yerleştirip içindeki verileri bilgisayara yüklemek şeklinde yapılabileceği gibi; internet üzerinden veri yüklemek şeklinde de gerçekleştirilebilecektir. Sisteme yerleştirilen veriler, daha sonra

1072 Taşdemir, age.

1073 8.CD. 24.06.2013 gün, 2012/32866-2013/18872. "Katılana ait hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturarak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suça sürüklenen çocuğun eyleminin TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması"

oluşturulan bir belgenin içeriğini etkilemişse, faili ayrıca belgede sahtecilikten de sorumlu tutan yargı kararları bulunmaktadır[1074].

fff) Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Göndermek

Burada, madde metninde açıkça ifade edildiği gibi bir bilişim sisteminde bulunan verilerin başka bir bilişim sistemine ya da veri taşıma aracına herhangi bir şekilde aktarılması, gönderilmesi hareketlerinden bahsedilmektedir. Bu hareketle veri ortadan kaldırılmamakta veya bütünlüğü bozulmaktadır. Bu hareketle sadece verinin, hak sahibi tarafından kullanılmasın engellenmektedir. Bilişim sisteminde var olan verilerin başka yere gönderilmesi eylemi internet ya da "wifi" gibi veri iletim ağları üzerinden 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.

244. maddenin 1 ve 2. fıkralarında düzenlenen suç seçimlik hareketli suçlardır. Maddede belirtilen seçimlik hareketlerden herhangi birisinin gerçekleştirilmesi durumunda suç oluşacaktır. Seçimlik hareketlerin birden fazlasının gerçekleşmesi halinde faile bir kez ceza verilecektir. Örneğin; verileri erişilmez kılma ve verileri değiştirme hareketlerinin aynı anda gerçekleşmesi gibi durumlarda tek suçtan ceza tayin edilecektir. Ancak burada da hakim TCK. nun 3 ve 61. maddeleri uyarınca alt sınırdan uzaklaşarak ceza tayin edebilecektir.

TCK'nın 243. maddesindeki bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren ve orada kalmaya devam eden kimse, kasten sistemdeki verileri bozar veya diğer seçimlik hareketlerden herhangi birisini gerçekleştirse, bilişim sistemine hukuka aykırı olarak girmek 244. maddenin 2. fıkrasında düzenlenen suçun unsuru olduğundan fail daha ağır ceza içeren 244/2. maddedeki suç nedeniyle cezalandırılacaktır.

cc) 244. Maddenin 4. Fıkrasındaki Eylem

Bu suçun oluşabilmesi için failin 244. maddenin 1. ve 2. fıkralarında belirtilen 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 ve gerçekleştirdiği eylemler neticesinde hukuka aykırı yarar, yasanın ifadesiyle

1074 "5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 10. maddesinde yer alan "Elektronik ortamda hazırlanacak bilgi ve belgeler adli ve idari makamlar nezdinde resmi belge olarak geçerlidir." şeklindeki düzenleme karşısında sanığın bir başkasına ait şifreyi kullanarak çalışmayan kişilerin çalışmaya başladıkları yönünde e-bildirge hazırlaması şeklindeki eyleminin resmi evrakta sahtecilik suçunu oluşturup oluşturmaycağı tartışılmadan yazılı şekilde karar verilmesi," (8. CD. 12.12.2013, 31922-29069)

"haksız bir çıkar sağlaması" gerekmektedir. Haksız çıkar ifadesiyle kastedilen *"hukuka aykırı yarardır"*. Yani 244. maddenin 1. ve 2. fıkrasındaki seçimlik hareketlerden bir veya daha fazlasını gerçekleştiren fail, fiilinin neticesinde haksız bir çıkar sağlamış ise bu durumda sanık hakkında 244. maddenin 4. fıkrası gereğince ceza tayin edilecektir. 244. maddenin 1. ve 2. fıkralarında düzenlenen eylemler 244. maddenin 4. fıkrasında düzenlenen suçun da eylem unsurunu oluşturmaktadır.

Failin gerçekleştirdiği eylemin sonucunda hukuka aykırı yarar elde edememesi durumunda 244. maddenin 4. fıkrasında düzenlenen suç oluşmayacaktır. Bu durumda 244. maddenin 1. ve 2. fıkralarında yer alan suçların gerçekleşmesi söz konusu olabilecektir.

244. maddenin 4. fıkrasında hukuka aykırı olarak çıkar maddi bir yarar olabileceği gibi bazı yazarlara göre tamamen duygulara hitap eden manevi bir yarar da olabilir. Haksız çıkarın mutlaka maddi olması şart değildir. Yasa metninde de çıkarın mutlaka maddi olması gerektiğine işaret edilmemiştir. Yargıtay 8. Ceza Dairesi öğrenci notunun yükseltilmesini ya da devamsız gün sayısının azaltılmasını TCK.nun 244/4 kapsamında "haksız çıkar" olarak değerlendirmemiştir. (Y. 8. CD. 08.01.2014, 2014/33044, 2014/236, 15.02.2017 2016/3794, 2017/1405) Suçun oluşabilmesi için failin sağladığı çıkarın haksız olduğunun farkında olması da zorunludur[1075]. Fail hukuka aykırı yararı kendisine ya da üçüncü şahsa sağlayabilir. Hukuka aykırı çıkarın elde edilmesiyle suç tamamlanacaktır.

Ancak 244. maddenin birinci ve ikinci fıkralarında belirtilen fiilleri işleyen failin, kendisine veya başkasına haksız bir yarar sağlamasının başka bir suç oluşturmaması gerekir. Eğer eylem başka bir suçu oluşturuyorsa artık fail hakkında gerçekleşen bu eylemden dolayı ceza tayin edilecektir. Örneğin gerçekleşen eylemin, dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne dayanılarak ceza tayin edilemeyecektir. Bu hükmün uygulanmasında suçun hukuki konusu çok önem arz etmektedir. Bu suçun hukuki konusu veridir. Veri taşınabilir mal değildir. Taşınabilir mal ancak hırsızlık gibi mala karşı suçların hukuki konusunu oluşturabilir.[1076] Bu genel kuralın istisnası olan TCK.nın 142/2-e maddesindeki

1075 Taşdemir, age.

1076 Y.11.CD. 18.09.2013 gün, 2012/2764- 2013/13257. "Katılanların ortağı ve yöneticisi oldukları Ef Turizm Organizasyon Hizmetleri ve Seles Kongre Organizasyon Ticaret Limited Şirketinin sigortalı çalışanları olan sanıkların, mülkiyeti anılan şirketlere ait olup sanıkların kullanımına bırakılan bilgisayarlardan, şirketlerin faaliyet alanları nedeniyle gelen e-mail tekliflerini ve müşteri portföylerini kopyalayarak şahsi e-mail adreslerine aktardıkları gibi mevcut bilgisayarlardan bu teklif e-mail'lerini silerek daha sonra kendilerinin ortak olarak kurdukları şirketleri olan 3 Gen Turizm Organizasyon Ltd. Şirketine aktardıkları somut olayda, suça konu verilerin güveni kötüye kullanma suçunun konusunu oluşturan eşya kavramı içerisinde değerlendirilemeyeceği de dikkate alındığında, 5237 sayılı TCK'nun 244/2-4. maddesinde yazılı "bilişim suçunu" oluşturduğu gözetilmeden, sanıkların eylemlerinin aynı

düzenleme karşısında failin bir başkasının interaktif banka hesabına internet yoluyla girerek kendi hesabına para (veri) transfer etmesi halinde TCK.nun 142/2-e maddesinde düzenlenen "'bilişim suretiyle hırsızlık" suçu oluşacaktır[1077]. Yine failin içerisinde mal bulunan bir deponun şifreli kilidinin bilişim sistemi kullanılarak açılması suretiyle içeriden mal çalınması durumlarında TCK. nun 142/2-e maddesinde düzenlenen bilişim sistemleri aracı kılınarak hırsızlık suçu gündeme gelecektir. Bu halde artık 244. maddenin 4. fıkrası uyarınca hüküm kurulamayacaktır.

Ceza Genel Kurulunun 2009/11-193, 2009/268 sayılı kararında "...sanığın, katılan şirketin banka hesabının internet şifresini kırarak bu hesaptan kendi hesabına havale yaparak haksız menfaat sağlamak şeklindeki eyleminin 5237 sayılı Yasanın 142/2-e maddesine uyduğu" kabul edilmiştir.

Dolandırıcılık suçunda da suçun hukuki konuları insan iradesinin özgürlüğü ve malvarlığına ilişkin varlık ve menfaatlerdir. Dolandırıcılık suçunda, bir şeyin teslimi, hile ile sakatlanmış ve özgür olmayan bir iradeye dayanmaktadır.

Dolandırıcılık suçunun oluşabilmesi için; failin bir kimseyi kandırabilecek nitelikte hileli davranışlarla hataya düşürüp onun veya başkasının zararına, kendisine veya başkasına yarar sağlaması gerekmektedir. Dolandırıcılık suçunun oluşabilmesi için; failin bir kimseyi kandırabilecek nitelikte hileli davranışlarla hataya düşürüp onun veya başkasının zararına, kendisine veya başkasına yarar sağlaması gerekmektedir. Dolandırıcılık suçunda hileli hareketin gerçek kişiye yöneltilmesi gerekmektedir. Eğer hileli hareketle bir bilişim sistemi yanıltılarak haksız yarar elde edilmesi halinde dolandırıcılık suçu oluşmayacaktır. Bu durumda 244. maddenin 4. fıkrası gündeme gelecektir[1078].

Yukarıda da bahsedildiği gibi 244. maddenin 4. fıkrasında düzenlenen suç tali norm niteliğindedir. Bu hükmün uygulanabilmesi için fiilin başka bir suçu oluşturmaması gerekmektedir. 244. maddenin 1. ve 2. fıkralarında belirtilen fiillerin gerçekleşmesi durumunda haksız bir yarar da elde edilmiş ise bu durumda eylemin dolandırıcılık, hırsızlık, güveni kötüye kullanma gibi başka bir suçu oluşturup oluşturmadığı araştırılmalıdır. Eğer eylem bu suçlardan birini oluşturuyorsa artık

Kanunun 155/2. maddesinde düzenlenen "hizmet nedeniyle güveni kötüye kullanma" suçunu oluşturduğundan bahisle yazılı şekilde hüküm tesisi;"

1077 CGK. 17.11.2009 gün ve 193/268 sayılı karar.

1078 **Y.8.CD. 24.12.2012 gün, 2012/21826-2012/39370**."Oluşa ve dosya kapsamına göre, mağdure F.Ç.'nun işvereni olan A.Y.'ün facebook şifresini bir şekilde ele geçiren sanığın, bu adresten mağdure ile A. A. gibi yazışarak 700 TL'lik kontör kartı aldırıp şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına yüklemesi şeklinde gerçekleşen eylemin, TCK.nun 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu oluşturabileceği ve bu suça bakma ve delilleri takdir etmenin ağır ceza mahkemesine ait olmasına karşın, görevsizlik kararı verilmeyerek yargılamaya devamla yazılı şekilde hüküm kurulması,

244. maddenin 4. fıkrası uygulanmayacaktır. Eylem bu suçlardan birisinin tanımına uymuyorsa, o zaman 244. maddenin 4. fıkrası hükmü uygulanabilecektir. 244. maddenin 4. fıkrası ancak eylemin başka bir suçu oluşturmaması halinde uygulanabilecektir. Örneğin eylem hırsızlık suçunu oluşturuyorsa artık TCK. nun 244/4. maddesi ile hüküm kurulmayacak, sadece oluşan hırsızlık suçundan hüküm kurulacaktır.[1079].

Ceza Genel Kurulunun 2013/13-448, 2014/524, 2015/15-867, 2013/13, 2012/15-1293, 2013/11 ve 2015/23-1100, 2015/10 sayılı kararlarında "www.arabam.com, www.srexi.com" gibi aynı anda birçok kişiye ulaşmada çabukluk ve kolaylık sağlayan bilişim sistemlerine yanıltıcı ilanlar verilerek gerçekleştirilen dolandırıcılık fiillerinin TCK.nın 158/1-f maddesi kapsamında kaldığı kabul edilmiştir.

Ancak, Ceza Genel Kurulu sanığın müştekiyi telefonda söylediği nitelikli yalanla ikna ettikten sonra istediği peşinatı internet bankacılığı yoluyla kendisine gönderilmesini istemesi ve müştekinin de bu şekilde parayı göndermesinde dolandırıcılıkta araç olarak kullanılanın telefon olup, bankanın bilişim sisteminin araç olarak değil, ödeme aracı olarak kullanıldığı gerekçesiyle eylemin TCK.nın 157/1. maddesinde tanımlanan suçu oluşturduğuna karar vermiştir. (CGK. 10.05.2016 gün, 2014/15-288, 2016/255)

Yargıtay 8. Ceza Dairesi kararlarında bilişim sisteminde bulunan ve mağdura ait oyun karakterlerini rızası haricinde alarak kendi ya da başkasının hesabına aktaran failin eylemini daha önceleri hırsızlık olarak değerlendirmiş ise de (2015/14257, 2016/1702) son olarak hırsızlık suçunu değil TCK.nın 244/2. maddesinde tanımlanan suçu oluşturduğuna karar vermiştir.(8. C.D. 2017/897 2017/6019, 2017/1283-14186)

Mali müşavir olan sanığın hiçbir işyerinde çalışmayan kişileri çalışıyor göstermek için şifre ve imza kullanarak Sosyal Güvenlik Kurumuna ait sisteme girerek e-bildirge oluşturması durumunda eylemi hangi suçu oluşturacaktır?

Yargıtay 8. Ceza Dairesine[1080] göre 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunun 100. Maddesi ile birlikte değerlendirildiğinde eylemin TCK'nın 204. maddesindeki sahtecilik suçunu oluşturduğunun kabulü gerekecektir.

1079 Y.2.CD. 19.06.2014 gün, 2014/22676-2014/17536."Sanıkların, katılanın banka hesabına bilgisi dışında intemet yoluyla erişim sağlayarak, hesabındaki parasını sanık Ş. T.'in hesabına havale etmeleri şeklinde gerçekleştiği kabul edilen eyleminin 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen hırsızlık suçunu oluşturduğu gözetilmeden, yazılı şekilde aynı Kanunun 244/4 maddesi uyarınca hüküm kurulması."
1080 Y. 8. CD. 12.12.2013, 31911-29069

Ancak Yargıtay 11. Ceza Dairesi[1081] ise; TCK'nun 244/2. maddesindeki sisteme veri yerleştirme suçunu oluşturduğunu kabul etmektedir.

Ceza hükmü içeren başkaca özel kanunlarda "*ayrıca düzenlenmiş olmadığı sürece*", elektronik ortamdaki verilerin ceza hukuku anlamında "*belge*" olarak kabul edilmeleri ve ceza hukuku korumasından yararlanmaları mümkün değildir. Dolayısıyla, bilgisayar sistemine hukuka aykırı olarak girilerek gerçeğe aykırı olarak verilerin sisteme yüklenmesi veya değiştirilmesi halinde, ortada fiziki anlamda bir belge mevcut olmadığı için, fiil TCK md. 204 vey 207'de tanımlanan suçları oluşturmayacaktır. Belirtilen eksiklik nedeniyle, bilgisayarlarla ilişkili sahtecilik fiillerinin resmi veya özel evrakta sahtecilik suçunu değil, TCK.nun 244/2. maddesinde düzenlenen verelire değiştirme veya yok teme suçunu oluşturmakta, bu da –*yaptırım açısından*- doktrinde bir tür ödüllendirme olarak nitelendirilmektedir. Kısacası TCK, elektronik ortamda gerçekleşecek sahtecilik fillleri yönüyle Sözleşme'de öngörülen yükümlülükleri karşılamaktan uzaktır[1082].

3. Suçun Nitelikli Hali:

Maddenin 1. ve 2. fıkralarındaki eylemlerin bir banka veya kredi kurumuna[1083] ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi ağırlatıcı neden olarak düzenlenmiştir. Ancak bu fıkranın uygulanabilmesi için bilişim sisteminin bir banka veya kredi kurumuna ya da bir kamu kurum ve kuruluşuna ait olması gerekir. Belirtilen ağırlaştırıcı nedenin gerçekleşmesi durumunda, faile verilecek ceza yarı oranında artırılacaktır. Örneğin failin ÖSYM'nin bilişim sistemine ya da öğrenim gördüğü okulun bilişim sistemine girerek kendi sınav sonuçlarını değiştirmesi gibi[1084].

1081 Y. 11. CD. 03.12.2015 gün, 10595-31550, 27.11.2017, 2015/8801, 2017/8230

1082 Arslan, Prof. Dr. Çetin, Baştürk, İhsan, Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Veriler, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, cilt VIII, sayı:2, yıl:2013, s.209,210

1083 5411 sayılı Bankacılık Kanunu'nun 3. maddesinde "Kredi kuruluşu: Mevduat bankalarını ve katılım bankalarını", "Banka: Mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını" ifader eder şeklinde tanımlama yapılırken "Mevduat bankası: Bu Kanunua göre kendi nam ve hesabına mevduat kabul etmek ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini", "Katılım bankası: Bu Kanuna göre özel cari ve katılma hesapları yoluyla fon toplamak ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini", "Kalkınma ve yatırım bankası: Bu Kanuna göre mvduat veya katılım fonu kabul etme dışında; krdei kullandırmak esas olmak üzere faaliyet gösteren ve/veya özel kanunlarla kendilerine verilen görevleri yerine getiren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini" ifade eder şeklinde de tanımlamalara devam edilmiştir.

1084 **Y.8.CD. 29.04.2014 gün, 2013/9376-2014/10958**. "Sanığın, katılana ait eczane şifresiyle S.G.K.'nun bilişim sistemine girerek katılanın eczanesi adına kayıtlı reçete bilgilerini silme şeklindeki eylemi nedeniyle hükmolunan cezanın S.G.K.'nun kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiğinin gözetilmemesi karşı temyiz bulunmadığından bozma nedeni yapılmamıştır."

Bu nitelikli halin uygulanabilmesi için suçun konusunu oluşturan bilişim sisteminin bankaya, kredi kurumuna, kamu kurumu veya kuruluşuna ait olması gerekir. Bu kurumlara ait bir bilişim sisteminin işleyişinin engellenmesi, bozulması bu sistemdeki verilere yönelik müdahalelerde bulunulması halinde ceza artırılacaktır. İfade edelim ki buradaki banka veya kredi kurumunun kamuya ait olması gerekmemektedir. Özel bir bankanın bilişim sistemine yönelik zarar verici fiiller bakımından da bu nitelikli hal gerçekleşir. Ancak diğer kurum veya kuruluşların "kamu kurum veya kuruluşu" olması şarttır. Böylece suçtan zarar görenin sıfatına göre bir nitelikli hal kabul edilmiş olmaktadır[1085].

4.Suçun Manevi Unsuru

TCK.nun 244. maddesinde düzenlenen suçlar genel kasıtla işlenebilen suçlardır. Özel kast aranmaz. Kast, doğrudan kast olabileceği gibi, olası kast da olabilir. Failin maddede belirtilen hareketleri kasten yapması yeterlidir. Yasada açıkça suçun taksirle işlenebileceği belirtilmediği için suçun taksirle işlenmesi mümkün değildir. Ancak 244. maddenin 2. fıkrasında tanımlanan hareketlerin gerçekleştirilmesiyle sistemin işleyişinin engellenmesi veya bozulması da mümkün olabilmektedir. Bu durumda da failin eyleminin hangi fıkraya göre cezalandırılacağının belirlenmesinde suçun unsuru olarak belirtilmemişse de faildeki amacın belirlenmesi gerekecektir[1086].

5.Hukuka Aykırılık Unsuru

244. maddedeki eylemlerin, hukuka aykırı olarak gerçekleştirilmesi yeterlidir. Bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile sistemin çalışması korunurken, verilerin yok edilmesi veya değiştirilmesi suçu ile veriler üzerinde tasarruf yetkisi bulunan kişinin, verilere her hangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanmasındaki çıkarı korunduğundan, söz konusu bu hakların sahibinin ya da yetkilisinin rızası, hukuka uygunluk sebebini oluşturacaktır. Yani sahibinin veya kullanıcısının rızası, hukuka aykırılığı ortadan kaldıracaktır. Ancak bu rızanın fiilin işlenmesinden önce olması gerekir. Fiilin gerçekleşmesinden sonraki rıza fiili hukuka uygun hale getirmeyecektir.

6.Suçun Özel Görünüş Şekilleri

a.Teşebbüs

244. maddenin 1., 2. ve 4. fıkralarında düzenlenen suçlara teşebbüs mümkündür. Teşebbüs icra hareketlerine başlandıktan sonra bu hareketlerin yarıda kalması şeklinde olabileceği gibi suçun

1085 Koca, age, s.95,96
1086 Dülger, age, s.435

icrasına ilişkin bütün eylemler tamamlandıktan sonra suçun oluşumu için aranan netice meydana gelmeden failin elinde olmayan nedenlerle suçun gerçekleşmemesi şeklinde de olabilecektir.

Ancak 244. maddenin 4. fıkrasında düzenlenen suçta failin amacı haksız çıkar elde etmek olduğundan, failin verilere müdahale etmesine rağmen eylemi neticesinde haksız çıkar elde edememesi durumunda teşebbüs hükmünün uygulanabilmesi için failin haksız çıkar sağlama kastının ortaya konması gerekecektir. Failin kastının hukuka aykırı çıkar elde etmek olduğunun ortaya konamaması durumunda failin maksadına bakılacaktır. Failin maksadı yalnızca verilere veya sisteme zarar vermekse, bu durumda maddenin 4. fıkradaki suça teşebbüsten değil, 1. veya 2. fıkradaki suçun tamamlanmış halinden hüküm kurulacaktır. [1087]

b.İştirak

Madde metninde özel bir iştirak hükmüne yer verilmemiştir. Bu nedenle suçlara iştirak açısından bir özellik söz konusu olmayıp TCK.nun 37., 38., 39. ve 40. maddelerindeki suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir. Bu suçlara iştirak her zaman mümkündür.

c.İçtima

244. maddenin 1., 2. ve 4. fıkralarında düzenlenen bu suçların zincirleme şekilde işlenmesi mümkündür. Örneğin failin okuduğu üniversitenin sistemine farklı zamanlarda girerek ders notlarını değiştirmesi halinde zincirleme suç hükümlerinin uygulanması gündeme gelecektir [1088].

Burada en önemli bir sorun, 244. maddedeki suç oluştuğu zaman aynı zamanda TCK.nun 243/1. maddesindeki suçun da oluştuğu kabul edilecek ve ayrı ayrı cezalar mı tayin edilecek yoksa yalnızca TCK'nın 244. maddesindeki suçtan mı ceza verilecektir.

Yukarıda 243. maddenin uygulamasında da değinildiği gibi bu durumda geçitli suç hükümleri uygulanarak iki ayrı suçtan değil, yalnızca sonuç suçtan, yani TCK. nun.244. maddesi uyarınca ceza tayin edilecektir[1089]. Yani bir bilişim sistemindeki verileri değiştirmek isteyen fail, bu suçun icra hareketlerini gerçekleştirirken, sisteme de girmekte ve dolayısıyla 243. maddeyi de

1087 Dülger, age, s.451

1088 Y.8CD. 08.01.2014 gün, 2012/33044-2014/236.
1-Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması,
2-Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince arttırılması gerektiğinin gözetilmemesi.

1089 Artuk – Gökçen – Yenidünya, age., s.4664, Ankara 2009

ihlal etmektedir. Bu itibarla, failin bu suçlardan yalnızca en ağır cezayı gerektiren 244. maddedeki suçtan dolayı cezalandırılması gerekecektir[1090].

Bununla birlikte 15. Ceza Dairesi 15.11.2016 gün, 2016/3871-8608 sayılı ilamında "..sanık M.Ç'ın olay tarihinde annesi F.Ç'ın abonesi gözüktüğü 0 532... numaralı cep telefonu hattıyla müşteki Ç.D'ın e-posta adresine şifresini kırmak suretiyle müştekinin izni ve bilgisi olmaksızın erişim sağladığı ve müştekinin erişimini şifresini değiştirerek engellediği, ardından da kendisine müşteki Ç.D'ın arkadaşı P.N olarak tanıtarak para talep ettiği, müştekinin arkadaşı P. ile telefonla görüşerek söz konusu mailin P. tarafından gönderilmediği, P.'e ait mail adresinin başkalarınca ele geçirildiğini öğrenmesi üzerine para göndermediği, sanığın bu şekilde üzerine atılı suçu işlediğinin iddia edildiği olayda" hem dolandırıcılık (158/1-f) hem de bilişim suçu (244/2) işlediğine karar vermiştir.

Bu suçun diğer bir özelliği ise tali norm niteliğinde olmasıdır. Nitekim madde metninde suçun bu özelliğini ifade etmek üzere fiilin başka bir suçu oluşturmaması gerektiğinden bahsedilmiştir. Bu durumda bilişim sistemleri aracılığıyla haksız çıkar sağlama şeklinde bir olayla karşılaşıldığında, ilk önce fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet gibi başka bir suçu oluşturup oluşturmadığı araştırılmalıdır. Şayet olayın gerçekleştiriliş şekli bu suçlardan birisinin tanımına uygun ise, bu suçlar işlenmiş olacaktır. Gerçekleştirilen fiil bu suçlardan birisinin tanımına uymuyorsa, o zaman 244. maddenin 4. fıkrası hükmü uygulanabilecektir. "Asli normun önceliği ilkesi" gereğince, bir fiil hakkında asli ve tali norm şeklinde iki hüküm bulunuyorsa, asli norm öncelikle uygulanacaktır[1091].

TCK.nun 244. maddesinin 4. fıkrasının metnine göre bu fıkrada düzenlenen suçu oluşturan fiil aynı zamanda başka bir suç oluşturuyorsa, diğer suçun daha ağır ya da hafif olması dikkate alınmaksızın olayda diğer suçun hükümleri uygulanacaktır. Gerekçedeki aksine anlatıma rağmen maddenin 4. fıkrasında sözü edilen başka suçun cezasının daha ağır olması zorunlu değildir[1092].

Yargıtay Ceza Dairelerince; failin bilişim sistemine şifre kırarak kirip, buradan aldığı fotoğrafı yayınlayacağı tehditiyle para isteme şeklindeki eylemlerinin, şantaj, özel hayatın gizliliğini ihlal ve bilişim sistemine izinsiz girme suçlarını oluşturduğu ve gerçek içtima kurallarına göre her suçtan ayrı ayrı cezalandırılması gerektiğine (4. CD 18.03.2015 gün, 2014/2222, 2015/24755, mağdurun e-posta adresinden izinsiz olarak fotoğraflar ve video görüntüleri temin

1090 Taşdemir, age. aksi görüş Dülger age, sh 438
1091 Koca, age, s.97
1092 Dülger age, sh. 453

ederek katılanın arkadaşlarına göndererek ve arkadaşlarına gönderdiği fotoğraflar yanında katılana sövme içeren sözler sarfetmek eylemlerinde; 114/2, 125/2-1, 243/1. maddelerinde tanımlanan suçların oluştuğuna karar verilmiştir. (12. CD 03.01.2016, 2015/5933, 2016/277)

Yargıtay 8. Ceza Dairesinin kararlarında da belirtildiği gibi "Bilişim sistemleri aracılığıyla bir çıkar sağlandığında öncelikle bilişim sistemlerinin kullanılması suretiyle hırsızlık, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık, zimmet gibi bir başka suçun oluşup oluşmadığı tartışılmalı, eylem başka bir suçu oluşturmamışsa TCK.nun 244/4 maddesi irdelenmelidir. Örneğin şikayetçinin hesabına ilişim sistemi kullanılarak girmek suretiyle başka birinin hesabına şikayetçinin hesabından para havale etmek başka bir suçu (TCK m. 142/2-e) oluşturacağından TCK.nun 244/4. maddesi uyarınca mahkumiyet hükmü kurulamayacaktır[1093].

7.Yaptırım

TCK.nun 244/1. maddesinde öngörülen hürriyeti bağlayıcı ceza 1 yıldan 5 yıla kadar, 244/2. maddesinde ise 6 aydan 3 yıla kadar hapis olarak öngörülmüştür. Aynı maddenin 3. fıkrasında düzenlenen suçun nitelikli halinin gerçekleşmesi durumunda cezalar yarı oranında arttırılacaktır.

Bazen bilişim sistemindeki bir verinin değeri bilişim sisteminin kendisinden ya da işleyişinden daha değerli olabilir. Bu durumda hakim, TCK.nun 3 ve 61. maddesindeki argümanları kullanmalıdır.

TCK.nun 244/4 maddesinde düzenlenen bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçundan 2 yıldan 6 yıla kadar hapis ve birlikte 5000 güne kadar adli para cezası öngörülmüştür.

B- SORUŞTURMA VE KOVUŞTURMADA DİKKAT EDİLMESİ GEREKEN HUSUSLAR

Bu madde kapsamında genellikle;

- (Facebook, twitter, instagram gibi) sosyal paylaşım sitesi hesabının şifresinin ele geçirilmesi, değiştirilmesi, hesabın kullanılamaması,

- Hesaptan bilgilerin ve resimlerin ele geçirilip sahte hesap açılması, hesap sahibinin yakınlarına arkadaşlık isteğinin gönderilmesi ya da hakaret içerikli iletiler gönderilmesi,

- Sahte hesap açılıp başkasına ait resmin kullanılması, hesapta başkalarının telefon numaralarının yazılması, bu şahsın fuhuş yaptığına dair ibarelerin eklenmesi,

- Hesabın ele geçirilerek hesap sahibinin arkadaşlarından zor durumda olduğu gerekçesiyle borç istenmesi ya da bir alışveriş merkezinden çekilişe katılacakları söylenip hile ile cep telefonu

1093 8. CD. 21.05.2018, 1115-5608

ya da kredi kartı bilgileri alınıp harcama yapılması, cep telefonlarına ücretlendirme doğruacak işlem yapılması,

- Şirkete ait web sitesinin ele geçirilmesi, hesabın iadesi için para talep edilmesi,

- Şirkete ait hesap bilgilerinin eski çalışanın yetkisiz erişimi ile ele geçirilmesi, yeni çalıştığı rakip firmada aleyhe kullanılması,

- Okulun web sitesine girilerek ders notlarına müdahale edilmesi, sisteme erişimin engellenmesi, sitede bulunan öğrenci bilgilerinin başka yerlere gönderilmesi gibi iddialarla gündeme gelmektedir.

Örneklerden görüldüğü üzere TCK 244. maddesi yanında başka suçlar (TCK 134, 136, 158/1-f maddeleri) da gündeme gelebilmektedir.

Sisteme girme ve kalmaya devam etme suçunda uygulandığı üzere, bu suçlarda da özellikle soruşturma aşamasında kaybolacak deliller gecikmeksizin ve hukuka uygun olarak toplanmalıdır.

Sistemin işleyişine ya da içeriğine müdahale ile işlenen bu suçlarda suçun konusu olan sistem ve içeriği son derece önemlidir.

Müdahale edildiği söylenen sistem üzerinde herhangi bir değişiklik yapılmadan gerekli incelemenin yaptırılması, sisteme ya da içeriğine zarar verilip verilmediği, verilmiş ise ne şekilde gerçekleştiği (virüs, solucan, trojen vs.), bilgi aktarılmış ise nereye aktarıldığı, başkasına yarar sağlanıp sağlanmadığı, (banka hesabından para transferi, cep telefonuna ya da internet faturasına ücret yansıtılması gibi) bu işlemler sırasında sisteme düşen IP adresi server ve log kayıtları üzerinde yapılacak inceleme ile tespit edilmeye çalışılmalıdır.

"…. İnternette kişisel amaçlı bilgi ve paylaşım için açtığı siteyi çalıştırmak için internet üzerinden sponsor hosting hizmeti veren şikayetçiye ait olan "Türkmmo" adli siteden "CnnTurk" niki ile 23.09.2013 günü sponsor host istediği, onun da internet üzerinden gönderdiği, hostu alan ve olay günü "voLk4n" niki ile subdomain açıp shell adlı zararlı kodları şikayetçiye ait siteye yükleyerek hosting hizmeti verdiği siteleri hackleyip zarar verildiği iddiasıyla açılan davada, şikayetçinin dilekçesi ekinde biraz ettiği deliller dışında delil toplanmamşıtır. Şikayetçinin ve suça sürüklenen çocuğun bilgisayarları üzerinde suç tarihine ilişkin LOG kayıtlarının karşılıklı olarak incelenmesi, suç tarihinde şikayetçinin sitesine izinsiz giriş yapan IP numaralarının ilgili servis sağlayıcısından tespiti, bilişim sistemindeki verilerin bozulup bozulmadığı, yok edilip edilmediği, değiştirilip değiştirilmediği veya erişilmez kılınıp kılınmadığı, sisteme veri yerleştirilip yerleştirilmediği, var olan verilerin başka bir yere gönderilip gönderilmediği saptanıp sonucuna göre, TCK.nun 244/2. maddesinde düzenlenen suçun oluşup oluşmadığı da değerlendirilerek suça

sürüklenen çocuğun hukuki durumun takdir ve tayini gerekirken, eksik incelemeye ve herhangi bir somut veriye dayanmadığı anlaşılan bilirkişi raporuna dayanarak yazılı şekilde hüküm kurulması, Yasaya aykırı, (BOZULMASINA)" (8. CD. 18.03.2015 gün, 2014/26822 E-2015/13964K)

Sisteme düşen IP adresi kullanıcısı ilgili servis sağlayıcı şirketten (Türk Telekom, Turkcell, Avea, Vodafone, Superonline vs.) sorularak tespit edilebilir ise de, uygulamada yurt dışı kaynaklı IP adresi ya da NAT uygulamasında kullanılan (ağ adresi dönüşüm uygulamasında kullanılan) IP adresi olması, kaynak IP ve port bilgisine ihtiyaç duyulması gibi nedenlerle kullanıcıya ulaşılamamakta ya da daha önce vurgulandığı üzere toplu kullanım alanlarında sisteme girilmesi nedeniyle failin tespiti imkansızlaşmaktadır.

Bu durumda şüphelenilen şahıs varsa onun kullandığı dijital materyaller üzerinde inceleme yapılması, ayrıca lehine yarar sağlanan kişi ya da kişiler yönünden de araştırma yapılması gerekmektedir. Ancak bu da kesin çözüm değildir. Keza lehine yarar sağlanan kişilerin de çoğu zaman eylemden haberdar olmadıkları, örneğin bir banka hesabından kendi hesabına para transferi yapılan şahsın bu eylemden haberdar olmadığı, zira menfaatin daha sonra bir başka hesaba ya da (sahte isimle başkası adına çıkartılmış) cep telefonuna aktarıldığı görülmektedir.

Şüpheliye ait dijital materyallerde inceleme yapılırken olay tarihi ve zamanı tüm ayrıntısıyla tespit edilmeli, hangi kullanıcı ile internete bağlandığı, olaya ilşikin veri olup olmadığı belirlenmeli, yine müşteki ya da başkalarına ait benzer kişisel ya da hesap bilgileri olup olmadığı, şifre kırıcı programın kullanılıp kullanılmadığı ya da başka kullanıcılar ile benzer konularda bağlantı kurulup kurulmadığı araştırılmalıdır.

Bir hesap bilgisine girilmesi ve ödeme yapılması (oyun satın alınması, telefon ya da internet faturası ödenmesi) gibi durumda sanal ortamda ödeme işlemleri yapan şirketler aracılığıyla işlem hakkında bilgi temini sağlanabilecektir.

Eğer lehine yarar sağlanan bir cep telefonu abonesi tespit edilebilirse, bu transferin hangi IP adresi üzerinden yapıldığı ve cep telefonu abone bilgileri ilgili GSM şirketinden temin edilebilecektir.

Eğer bir banka, şirket ya da kurumun bilişim sistemine girildiği iddiası varsa, öncelikle söz konusu banka/kurum/şirketten yapılan işlemin niteliği, sisteme ne şekilde girildiği, sisteme girildiği sırada düşen IP adresi tespit edilip edilemediği, bu işlem ile bilgi ya da para transferi olup olmadığı, yapılmış ise hangi cep telefonu, hesap ya da sisteme aktarıldığı hususları ayrıntılı olarak sorulmalıdır.

Bir başka hesaba ya da cep telefonuna para aktarılması söz konusu ise, bu paranın ne suretle harcandığı, nereden çekildiğ ilgili banka ya da GSM şirketinden sorulmalı, varsa kamera görüntülüri gecikmeden temin edilmelidir. Eğer bir bankadaki hesaptan başka hesaba para aktarma söz konusu ise, her iki hesabın bağlı olduğu bankalardan ayrıntılı bir şekilde hesap hareketleri istenmeli, şüpheli konumunda bulunan şahısların hesabına başka yerlerden de benzer para transferi olup olmadığı incelenmelidir.

C.TCK. NUN 244. MADDESİ İLE İLGİLİ YARGITAY KARARLARI

1.Sanığın, katılana ait eczane şifresiyle S.G.K.'nun bilişim sistemine girerek katılanın eczanesi adına kayıtlı reçete bilgilerini silme şeklindeki eylemi nedeniyle hükmolunan cezanın S.G.K.'nun kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiğinin gözetilmemesi karşı temyiz bulunmadığından bozma nedeni yapılmamıştır. (Y.8.CD. 29.04.2014 gün, 2013/9376-2014/10958)

2.Sanığın; SGK.nun bilişim sistemine girerek katılanın eczanesi adına kayıtlı reçeteleri sistemden silmek şeklindeki eylemi nedeniyle hükmolunan cezanın SGK.nun kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden, yazılı şekilde hüküm kurulması aleyhe temyiz bulunmadığından bozma nedeni yapılmamıştır. (Y.8.CD. 15.04.2014 gün, 2013/9180- 2014/9692)

3.Sanık hakkında düzenlenen ve davanın temelini oluşturan 23.09.2011 tarihli iddianamede; "şüphelinin, şikayetçinin arkadaşı olan Fatma'ya ait mail adresini ele geçirerek, şikayetçi ..... ile yazışıp ona cinsel taciz ve tehditte bulunduğu belirtilerek" dava açılmış olup, CMK.nun 225. maddesi uyarınca hükmün konusunun iddianamede açıklanan fiil olduğu, iddianamede yer almayan olaylara ilişkin yargılama yapılamayacağı gözetilmeden sulh ceza mahkemesinin iddianame kapsamı dışına çıkarak "sanık tarafından şikayetçinin msn ve facebook şifrelerini ele geçirip değiştirilerek erişimin engellendiği, şikayetçinin başka bir mail adresi edinerek, sanıkla iletişime geçtiğinde, sanığın tehdit, hakaret ve cinsel tacizde bulunduğundan" bahisle verdiği görevsizlik kararına dayanılarak ve bilişim sisteminin ne şekilde engellendiği ve değiştirildiğine ilişkin kanıtların neler olduğu da kararda gösterilip tartışılmadan TCK.nun 244/2. madde ve fıkrası ile mahkumiyet hükmü kurulması, (24.09.2013. 2012/30296- 2013/23181 SB. 8. CD)

4.5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 100. maddesinde yer alan "Elektronik ortamda hazırlanacak bilgi ve belgeler adli ve idari makamlar nezdinde resmi belge olarak geçerlidir." şeklindeki düzenleme karşısında sanığın bir başkasına ait şifreyi

kullanarak çalışmayan kişilerin çalışmaya başladıkları yönünde e-bildirge hazırlaması şeklindeki eyleminin resmi evrakta sahtecilik suçunu oluşturup oluşturmayacağı tartışılmadan yazılı şekilde karar verilmesi, (Y.8. CD. 12.12.2013. 2012/31922-2013/29069.)

5.Katılana ait hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturarak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suça sürüklenen çocuğun eyleminin TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması, (Y.8. CD. 24.06.2013 gün, 2012/32866-2013/18872)

6.Oluşa ve dosya kapsamına göre, mağdure F.Ç'nin işvereni olan Av.A.A'nın facebook şifresini bir şekilde ele geçiren sanığın, bu adresten mağdure ile A.A gibi yazışarak 700 TL'lik kontör kartı aldırıp şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına yüklemesi şeklinde gerçekleşen eylemin, TCK.nun 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu oluşturabileceği ve bu suça bakma ve delilleri takdir etmenin ağır ceza mahkemesine ait olmasına karşın, görevsizlik kararı verilmeyerek yargılamaya devamla yazılı şekilde hüküm kurulması, (24.12.2012. 2012/21826-2012/39370. SB. Y. 8. CD)

7.Oluşa ve dosya kapsamına göre; şikayetçiler K.T, Z.V, Ö.Ş isimli kişilere ait msn adreslerini kırarak ilgili adreslerdeki kişilerin arkadaşlarından onlarmış gibi yazışarak kendine yarar sağlamak amacı ile kontör talep edip şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına yüklemesi şeklinde gerçekleşen eylemin, TCK.nun 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu oluşturup oluşturmayacağına ilişkin delilleri takdir ve tartışmanın 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 12. maddesi uyarınca ağır ceza mahkemesinin görevinde bulunduğu gözetilerek görevsizlik kararı verilmesi gerekirken, yargılamaya devamla yazılı biçimde hüküm kurulması, (Y. 8. CD. 18.12.2013. 2013/735- 2013/29491 SB.)

8. 1-Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması,

2- Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince arttırılması gerektiğinin gözetilmemesi, (Y. 8. CD. 08.01.2014. 2012/33044- 2014/236. SB.)

9.Sanık E.A'nın, internet platformu hazırlamak ve işletmek amacıyla faaliyet gösteren katılan şirket bizimalem.com adlı bir site ile arkadaş bulmak, forumlarda bilgi alışverişi yapmak, sohbet etmek, oyun oynamak üzere üye kaydı esasına göre çalışan bir sistemine girip onun işleyişini engellediği, kayıtlarını ve bazı bilgilerini başka bir siteye aktardığından bahisle açılan davada, sanığın suçlamayı kabul etmediği, sitenin kendisine iş teklif ettiği, bu nedenle hesap numarası istendiğinde kendisinin bir bankada hesabı olmadığından tanıdığı olan internet cafe sahibinin hesabını bildirdiğini, daha sonra kendisine gönderilen sözleşmenin sözlü anlaşmaya uygun olmadığını görünce vazgeçtiğini, bu nedenle kendisine iftira atıldığını savunması, mahkemece alınan bilirkişi raporunda yukarıdaki fiillerin başkasına ait internet cafeden gerçekleştirildiğini, anılan web sitesinin işletim sistemine girmek, çökertme işlemlerinin gerçekleştirilmesinin zor olup uzmanlık veya şans gerektirdiği, internet cafeye ait bilgisayarların hard diskleri üzerinde yapılan incelemede yabancı MSN, Hotmail kullanıcılarının olduğunun saptandığı, bunun amacının, katılana ait site üyelerini sanığın sitesine yönlendirme ve tüm bilgilerini buraya aktarmak olduğu, katılan şirket yöneticisi ile sanığın görüntülü görüşmelerinin bulunduğu belirtilmiş ise de dosya içindeki belgeler arasında sanığın görüntüsünü içeren bir belgeye rastlanmadığı gibi yapılan işlemleri açıklamaktan uzak olduğu dikkate alındığında, bu konuda uzman bilirkişi heyeti vasıtasıyla yeniden inceleme yapılarak sanığın atılı suçu işlediğine ilişkin delillerin kesin olarak neler olduğunun saptanması gerekirken yetersiz bilirkişi raporuna dayanarak yazılı şekilde hüküm kurulması, (Y.11. CD. 27.03.2013. 2011/5893-2013/5065)

10. Katılanların ortağı ve yöneticisi oldukları ..... Turizm Organizasyon Hizmetleri ve ..... Kongre Organizasyon Ticaret Limited Şirketinin sigortalı çalışanları olan sanıkların, mülkiyeti anılan şirketlere ait olup sanıkların kullanımına bırakılan bilgisayarlardan, şirketlerin faaliyet alanları nedeniyle gelen e-mail tekliflerini ve müşteri portföylerini kopyalayarak şahsi e-mail adreslerine aktardıkları gibi mevcut bilgisayarlardan bu teklif e-mail'lerini silerek daha sonra kendilerinin ortak olarak kurdukları şirketleri olan ..... Turizm Organizasyon Ltd. Şirketine aktardıkları somut olayda, suça konu verilerin güveni kötüye kullanma suçunun konusunu oluşturan eşya kavramı içerisinde değerlendirilemeyeceği de dikkate alındığında, 5237 sayılı TCK'nun 244/2-4. maddesinde yazılı "bilişim suçunu" oluşturduğu gözetilmeden, sanıkların eylemlerinin aynı Kanunun 155/2. maddesinde düzenlenen "hizmet nedeniyle güveni kötüye

kullanma" suçunu oluşturduğundan bahisle yazılı şekilde hüküm tesisi; (Y. 11. CD.18.09.2013 gün, 2012/2764- 2013/13257.)

11. Katılana ait hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturarak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suça sürüklenen çocuğun eyleminin TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması, (Y. 8.CD. 24.06.2013 gün,2012/32866-2013/18872)

12.TCK.nun 245/1. maddesinde yazılı suçun oluşabilmesi için, her ne suretle olursa olsun ele geçirilen bir kredi veya banka kartının ATM cihazında kullanılması yahut alışveriş yapılması, bu suça teşebbüs için de kartın kullanılmasına yönelik icra hareketlerine başlamış olması gerektiği cihetle,

Somut olayda; ATM'de tertibat aldıktan sonra kart yuvasına kurduğu düzenek sayesinde, şikâyetçinin kartının sıkışmasını sağladıktan sonra yardım bahanesiyle yaklaşıp, kartın şifresini öğrenmeye çalıştığı, şikâyetçinin durumdan şüphelenip şifresini vermemesi üzerine sanığın makinedeki düzeneği ve kartı çıkartıp şikâyetçiye vermek şeklindeki eylemde; kartın sıkışmasını sağlamak için yerleştirilen aparatın takılı olduğu süre boyunca bilişim sisteminin bir parçası olan ATM'nin kullanılamaması karşısında; gerçeğin ve suç niteliğinin kuşkuya yer vermeyecek şekilde belirlenebilmesi için ATM üzerinde gerçekleştirdiği hareketlerinin ayrıntılı olarak tespiti ile bu hareketin bir bilişim sisteminin parçası olan ATM'nin kısa süreliğine de olsa çalışmasına engel teşkil edip etmediği, bağlı bulunduğu bilişim sistemi veya cihaza bir zarar verip vermediği hususları ilgili banka şubesinden sorulup, bu hususta gerektiğinde bilirkişi raporu da alınarak, cihazın ait olduğu banka davadan haberdar edildikten sonra, sanığın hukuki durumunun takdir ve tayini gerektiği ve suça konu kartın sanık tarafından ele geçirilmediği ve kullanılmadığı gözetilmeden, eksik soruşturma sonucu yazılı şekilde hükümler kurulması, (Y. 8. CD.12.03.2014 gün, 2013/13519- 2014/6128) (Banka veya kredi kartlarının kötüye kullanılması ve hırsızlık suçlarından hüküm kuruldu)

13. 2797 sayılı Yargıtay Yasasının 6110 sayılı Yasa ile değişik 14. mad- desinde “Ceza Dairesinde, Daireler arasındaki işbölümünün belirlenmesinde, dava açılan belgedeki nitelendirme esas alınır. Açıklama ile sevk maddelerinin uyumsuz olduğu durumlarda, açıklamaya itibar edilir” hükmü yer almaktadır. Yasa, sevk maddelerine değil, iddianamedeki tavsife ağırlık tanımıştır. Bu nedenle Ceza Dairelerinin görevinde Ceza Daireleri Başkanlar Kurulunun yerleşik kararlarında da belirtildiği üzere tavsif esas alınmalıdır.

Adana Cumhuriyet Başsavcılığı'nın iddianamesine göre sanığın şikâyetçinin interaktif banka hesabına internet aracılığıyla girerek kendi hesabına para transfer edip çekmeye çalıştığının iddia olunması karşısında; Yargıtay Ceza Genel Kurulu'nun 17.11.2009 gün ve 193/268 sayılı kararında açıklandığı üzere 5237 sayılı TCK'nun 142/2-e maddesinde öngörülen "bilişim suretiyle hırsızlık" suçu tavsif edilerek dava açılmıştır.

Bu itibarla, iddianamedeki anlatıma, temyizin kapsamına ve Yargıtay Kanunun 14. maddesine göre temyiz inceleme görevinin Yüksek (2.) Ceza Dairesine ait olduğu anlaşıldığından; Dairemizin görevsizliğine, dosyanın görevli daireye gönderilmesine. (Y.8.CD.02.06.2014 gün, 2013/4709-2014/13494)

14.Oluşa ve dosya kapsamına göre, sanığın 20.09.2006 tarihinde İzmir/Bornova'da bulunup tanık V.A'nın tarafından işletilen internet kafeye giderek burada bulunan bilgisayarlardan biriyle gündüz sayılan saat 15:58-16:06 saatleri arasında yaptığı 7 ayrı internet bankacılığı işlemi ile, Akbank İstanbul/İstinye/Carrefoursa şubesindeki katılana ait banka hesabına bağlı internet şubesi hesabına katılanın bilgi ve rızası dışında girip hesaptaki döviz ve hazine bonolarını bozdurarak ve hesapta bulunan nakit parayı da kullanıp toplam 57.500 TL'yi aynı bankanın İzmir/Konak şubesinde bulunan kendi adına açtığı hesaba havale yoluyla aktardıktan sonra 21.09.2006 günü yine aynı bankanın Konak, Hatay ve Buca olmak üzere 3 ayrı şubesinden 20.000, 15.000 ve 22.500 TL şeklinde parça parça çektiği olayda; sanığın eyleminin 5237 sayılı TCK'nın 142/2-e düzenlenen bilişim sisteminin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden, eylemin vasıflandırılmasında yanılgıya düşülerek yazılı şekilde aynı Yasanın 244/4. maddesi ile hüküm kurulması. (Y.6. CD. 27.05.2014 gün, 2012/7246- 2014/10715)

15. Sanıkların haksız bir şekilde ele geçirdiği yakınana ait internet bankacılık şifresini kullanmak suretiyle, yakınanın Yapı Kredi Bankası Harput Şubesinde bulunan hesabından, sanık M.E.K'nin hesabına 2070 TL havale yapıp, bankamatik kartı ile sanık U.A tarafından paranın çekildiğinin anlaşılması karşısında; yakınanın banka hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanan sanıkların tamamlanan eylemlerinin Yargıtay Ceza Genel Kurulunun 17.11.2009 tarih ve 11-193/268 sayılı kararında da ayrıntıları açıklanan 5237 sayılı TCK'nın 142/2-e maddesine uyan suçu oluşturduğu dikkate alınmadan suçun vasfında yanılgıya düşülerek yazılı şekilde uygulama yapılması. (Y.6. CD. 30.06.2014 gün, 2012/3216- 2014/13608)

16.Sanıkların, katılanın banka hesabına bilgisi dışında internet yoluyla erişim sağlayarak, hesabındaki parasını sanık Ş.T'nin hesabına havale etmeleri şeklinde gerçekleştiği kabul edilen eyleminin 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen hırsızlık suçunu oluşturduğu

gözetilmeden, yazılı şekilde aynı Kanunun 244/4 maddesi uyarınca hüküm kurulması. (Y.2.CD. 19.06.2014 gün, 2014/22676-2014/17536)

17. Katılanın rızası olmaksızın ele geçirdiği kredi kartı bilgilerini internet üzerinden mail order yöntemiyle kullanan sanığın eyleminin bir bütün olarak TCK.nun 245/1. maddesinde düzenlenen banka veya kredi kartının kötüye kullanılması suçunu oluşturduğu ve suça konu eylemin işlendiği internet sitelerine yönelik hukuka aykırı bir fiil bulunmadığı gözetilmeden, TCK.nun 244. maddesinde düzenlenen ve olayda unsurları bulunmayan bilişim sistemine girme suçundan mahkumiyet kararı verilmesi, (Y.8.CD. 08.05.2014 gün, 2013/4704-2014/11881)

18- Katılana ait hotmail adresine hukuka aykırı olarak giren ve yeni şifre oluşturup katılanın erişimini engelleyerek e-mail adresini kullanan sanığın eylemine uyan TCK.nın 244/2. madde ve fıkrası uyarınca cezalandırılması gerektiği gözetilmeden yazılı şekilde beraat kararı verilmesi (Y. 8. C.D. 23.06.2014 gün, 2013/771- 2014/15833)

19- Şikayetçinin 01.11.2011 tarihinde internette KNİGHT ONLİNE WORLD isimli oyunu oynarken ....@hotmail.com.tr adresinden arkadaşlık teklifi geldiğini, bu teklifi kabul ederek karşıdaki şahısla bu adresten konuştuğunu, tekrar oyuna döndüğünde oyun şifresinin çalınıp oyun karakterlerinin aldığından bahisle açılan davada, sanığın suçlamayı kabul etmemesi, anılan mail adresini kullanmadığını savunması, adli bilişim büro amirliğinin 17.07.2013 tarihli imaj alma tutanağında, sanığın evinde mikro-2 GB SD kart üzerinde yapılan incelemede suç unsuruna rastlanılmadığının bildirilmesi, bilirkişi tarafından düzenlenen 01.04.2014 tarihli raporda, oyun şifresini çalacak kadar bilgi ve beceriye sahip bir kişinin işlemi yapmış olduğu, bilgisayarın kullandığı IP adresinin de sisteme düşeceğini bileceği değerlendirildiğinden suçu işlediği hususunda kanaat oluşmadığının belirtilmesi, microsoft şirketinden gelen cevapta ...@hotmail.com.tr adresine girenler arasında sanığa ait IP numarasına rastlandığı ancak başka IP numaralarının da olduğu halde araştırılmaması karşısında, anılan mail adresinin bilgilerinin bağlı olduğu şirketten sorulup, suç tarihinde kimin kullanımında olduğunun belirlenmesi, oyun sitesinden suç tarihinde, şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemin TCK.nun 244/4. maddesindeki suçu oluşturacağı da dikkate alınarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, (Y. 8. C.D. 25.05.2017 gün, 2017/897 – 6019)

20- Aşamalarda sanığın şifreyi değiştirdiğini beyan etmesi karşısında; şikayetçi A. B.'a ait Facebook ve e-mail adreslerine girerek şifreleri değiştirmek suretiyle erişilmez kılan sanığı neyleminin TCK.nın 244/2. maddesinde düzenlenen suçu oluşturacağı gözetilmeden aynı maddenin 1. fıkrası ile hüküm kurulması (8. C.D. 17.05.2017 gün, 2016/10061 - 2017/5649)

21- Sanığın G... Eczanesi sahibi, sanık H. B. ile M. C. G.'ün ise kalfa olarak çalıştıkları, Medula sistemini kullanmaya yetkili sanıklar H. B. ile M. C. G.'ün olay tarihlerinde kendi çalıştıkları G... Eczanesi'nin şifresi ve katılan A. T.'ya ait T.. Eczanesi'nin haksız şekilde elde ettikleri Medula sistemine giriş şifresi ile önce hayali bir reçetenin eczanelerden birinin şifresiyle ..... Eczane sistemine giriş yapıldığı, hayali reçete ..... Eczane Sistemine kayıtlı iken bu kez diğer eczanenin sisteminden giriş yapılarak gerçek reçetenin sisteme kaydedildiği, hayali reçetenin sisteme kaydedilmesi ile hasta muayene ücretinin çıktığı, ancak hayali reçete sistemde kayıtlı bulunduğu halde diğer eczaneden gerçek reçetenin girişi yapıldığında muayene ücretinin çıkmadığı ve reçetenin karşılandığı, bu kez gerçek reçete karşılandıktan sonra hayali reçetenin sistemden silindiği ve hastaya ait muayene ücretinin bu işlemle bir sonraki ilaç alışına kadar ötelenerek bilişim sistemindeki verileri bozma, yok etme, sisteme veri yerleştirme suçunu işlediklerinden bahisle açılan davada; sanıkların sübut bulan eylemlerinde, dosya kapsamından yapılan işlemlerin katılan kurumun alacağını geciktirmekten ibaret olduğu, ortadan kaldırmadığı, bu surette bir haksız menfaat elde edilmediğinin anlaşılması karşısında, katılan A.T.'ya ait eczanenin şifresini haksız ele geçirip bunun vasıtasıyla Sosyal Güvenlik Kurumu'na ait bilişim sistemine giriş yapıp sahte veri yerleştirip amacına ulaştıktan sonra silmek şeklindeki eylemin TCK.nun 244/2 ve 3. maddelerindeki suç kapsamında değerlendirilmesi gerektiği gözetilmeden anılan maddenin 4. fıkrasıyla hüküm kurulması, (Y. 8. C.D. 31.05.2017 gün, 2016/12437 – 2017/6369 benzer 2016/6938 – 9936)

22- Katılanlar Akbank ile Finansbank adlarına vekillerinin temyiz istemlerinin bankalarına ait bilişim sistemlerine girip sahte internet siteleri oluşturmak ve bu suretle müşteri bilgilerini elde ederek kayıt etmek suçlarına yönelik olduğu anlaşılmakla,inceleme bu suçlarla sınırlı olarak yapılmıştır.

Sanıkların Akbank TAŞ ile Finansbank AŞ. adlarına sahte internet siteleri oluşturup sahte site sayfası açarak katılan bankaların müşterilerine sahte e-mailler gönderilerek sahte oluşturulan internet sayfaları ile ilgili yanıltıcı bilgiler verilerek güncelleme VS adı altında kişisel bilgilerini ve şifrelerini girmelerini istedikleri, bilgisayar çıktısında liste halinde belirlenen birçok bankaların müşterisinin bu sahte e-maillere inanarak verilen kişisel bilgileri ve banka şifrelerini dosyası tefrik

olunan suça sürüklenen çocuk B.B.'ın e- mail hesaplarında depolamaktan ibaret eylemlerinin TCK.nun 244/2 ve 136. maddeleri kapsamındaki suçları oluşturduğu, sanıklara yüklenen suçların yasa maddelerinde öngörülen cezalarının türü ve üst sınırları itibariyle tabi oldukları 5237 sayılı TCK.nun 66/1-e maddesinde belirlenen 8 yıllık dava zamanaşımının, zamanaşımını kesen son işlem olan sanıkların savunmalarının alındığı tarihler olan 17.09.2008 ve 27.05.2009 tarihlerinden temyiz inceleme tarihine kadar gerçekleştiği anlaşılmış ve katılanlar vekillerinin temyiz itirazları bu nedenle yerinde görülmekle sair yönleri incelenmeyen hükümlerin 5320 sayılı Yasanın 8/1. maddesi gereğince uygulanması gereken 1412 sayılı CMUK.nun 321. maddesi uyarınca BOZULMASINA, ancak yeniden yargılama yapılmasını gerektirmeyen bu hususta anılan Yasanın 322. maddesinin verdiği yetkiye dayanılarak karar verilmesi mümkün olduğundan sanıklar hakkında açılan kamu davalarının gerçekleşen dava zamanaşımı nedeniyle 5237 sayılı TCK.nun 66/1-e ve CMK.nun 223/8. maddeleri gözetilerek DÜŞÜRÜLMESİNE, (Y. 8. C.D. 07.06.2017 gün, 2016/12067 – 2017/6651)

23- Şikayetçinin e-mail ve facebook hesaplarına ait şifrelerinin elde edilerek değiştirilmesi nedeniyle erişemediğini, bu şifrelerle oyun oynadığı sitedeki oyun karakterlerinin de çalındığını, daha sonra e-mail şifresini geri aldığını ancak facebook şifresini alamadığını belirterek şikayetçi olması, sanığın suçlamayı kabul etmeyerek, bilgisayardan anlamadığını, sadece oyun oynadığını, oğlunun da bilgisayarı kullandığını savunması, şikayetçinin mail adresine girenler arasında sanığa ait IP numarasına rastlandığı ancak başka IP numaralarının da olduğu halde evrakların tefrik olması nedeniyle Manisa Cumhuriyet Başsavcılığında bulunan soruşturmanın akıbetinin araştırılmaması karşısında, anılan mail ve facebook adreslerinin bilgilerinin bağlı olduğu şirketten sorulup, suç tarihinde kimin kullanımında olduğunun belirlenmesi, Manisa Cumhuriyet Başsavcılığı'nın 2014/731 soruşturma nolu evrakın akıbetinin sorulması, yetkisizlik kararı verilmişse ilgili Cumhuriyet Başsavcılığından bilgi istenmesi, sanığın oğlu T. D.'in CMK.nun 48. maddesi uyarınca dinlenmesi, şikayetçiden hangi oyun sitesinde oyun oynadığı ve çalındığı iddia olunan karakterleri sorulup ilgili oyun sitesinden suç tarihinde, şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemin TCK.nun 244/2 veya 244/4. maddelerindeki suçları oluşturup oluşturmayacağı değerlendirilerek sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, (Y. 8. C.D. 13.12.2017 gün, 2017/1283-14186)

24- Oluşa ve tüm dosya kapsamına göre; hakkındaki dosya tefrik edilen M.G'nin işletmekte olduğu, katılan kurum ile anlaşması olmayan fatura ödeme merkezinde kurulu bulunan bilgisayar üzerinden katılan kurumdan emekli vezne şefi A.A'ya ait kullanıcı kodu ve şifresi kullanılarak ASKİ'nin fatura ödemelerinin yapıl- dığı sistemine girildiğinin ve sanığa ait toplam 1027.40 TL tutarındaki faturaların öden- diğinin, sanığın ise borcundan dolayı kapalı olan su aboneliğine ait faturalarının kim tarafından ödendiğini bilmediğine yönelik suçtan kurtulmaya yönelik savunmada bulunduğunun anlaşılması karşısında sanığın atılı suçtan mahkumiyeti yerine yazılı şekilde beraatine hükmolunması, (Y. 8. CD 2013/12582, 2014/10065)

25- 08/01/2014 günü saat 14:30 sıralarında kurumsal ve resmi olarak kullandıkları "www.igdirkhb.gov.tr" web sitesine yönetim menüsü altında idari ve mali işler başkanı linkine tıkladığında normalde çalışması gereken sayfa olan "www.igdirkhb.gov.tr/idari.php'"nin açılmayarak bu sayfanın yerine "yilsan.net/index.html" isimli web sitesinin açıldığını, sitenin bu şekilde yönlendirildiğini, yönlendirilen sitede kuruma yakışmayan yazı, resim ve müziklerin olduğundan bahisle açılan davada, sanığın suçlamayı kabul etmemesi,şikayetçi idarenin internet sitesine girenler arasında sanığa ait IP numarasına rastlandığı ancak başka IP numaralarının da olduğu halde evrakın tefrik olması nedeniyle diğerlerinin Iğdır Cumhuriyet Başsavcılığı'nda bulunan soruşturmaların akıbetinin araştırılmaması karşısında, Iğdır Cumhuriyet Başsavcılığı'nın 2014/2212 soruşturma nolu evrakın akıbetinin sorulması, yetkisizlik kararı verilmişse ilgili Cumhuriyet Başsavcılıklarından bilgi istenmesi,dava açılmışsa dava dosyalarının getirtilmesi, incelenip birleştirilmesi, mümkün değilse bu davayı ilgilendiren delillerin onaylı örneklerinin dosyaya konulması, sonucuna göre sanığın atılı suçu işlediğine ilişkin şikayetçi kurum tarafından verilen LOG kayıtlarından saptanan IP numarası tespiti dışındaki delillerin varlığı da karar yerinde gösterilerek hüküm verilmesi gerekirken eksik incelemeye dayanarak yazılı şekilde karar verilmesi, (Y. 8. CD 2018/1759, 2018/2386)

26- Katılanın alt bayi olarak internet sitesi üzerinden kontör alım satımı ve fatura ödemeleri gerçekleştirmek üzere kendisine verilen şifre bilgilerini bilgisi ve rızası olmaksızın ele geçirerek kontör satışı gerçekleştirmekten ibaret eylemlerin TCK.nun 142/2-e maddesi kapsamındaki suçu oluşturacağı gözetilmeden ve bilişim sistemi üzerinde çalışmasını engelleyecek girişimde bulunup veri değiştirerek haksız menfaat elde ettiklerine dair delil bulunmadığı halde suç vasfından yanılgıya düşülerek yazılı şekilde hükümler kurulması,

Suç tarihi itibariyle 18 yaşını ikmal etmeyen suça sürüklenen çocuk hakkında 5237 sayılı TCK.nun 53/4. madde ve fıkrasına aykırı olarak aynı Yasanın 53/1. madde ve fıkrasında yer alan hak yoksunluklarına hükmolunması, (Y. 8. CD 2016/12723, 2017/5659)

27- ... oyun sitesine girerek katılanın gerek ücreti karşılığında gerekse level atlama şeklinde kazandığı oyun karakterini ele geçirmek şeklindeki eyleminin, sübutu halinde bilişim suretiyle hırsızlık suçunu oluşturacağı (8. CD 17.02.2016, 2015/14257, 2016/1702

28- Hakkı hükmün açıklanmasının geri bırakılması kararı verilen sanıklardan M.A'nın, e-bildirge ile bilgisayar ortamında sahte işe giriş bildirgesi düzenleyerek, işyerinde çalışmayan sanığı sigortalı olarak gösterdiği ve bu suretle iştirak halinde resmi belgede sahtecilik suçunu işlediklerinin iddia ve kabul olunduğu olayda; imza ve şifre ile bilgisayar ortamında işe giriş bildirgelerinin verilmesi eyleminde, sahte oluşturulmuş maddi ve somut bir belge olmadığı, eylemin bu hali ile TCK.nun 244/2. maddesinde yazılı "sisteme veri yerleştirme" suçunu oluşturduğu gözetilmeden, suç niteliğinde yanılgı ile yazılı şekilde resmi belgede sahtecilik suçundan hüküm kurulması, (11. CD 27.11.2017, 2015/8801, 2017/8230)

29- Sanığın katılanın telefon hafıza kartını bir şekilde ele geçirip facebook şifrelerini de kırarak bu hesabı kullanmaya başlayıp elde ettiği fotoğrafları facebooktan yaymaya başalayacağını söyleyerek kendisiyle görüşmeyed evam etmesi için kendine ait telefondan katılana ait telefona gönderdiği "elimde görüntülerin var, bunları yayınlayacağım", "faceteki resimleri beğendiysen değiştireyim mesela oteldeki faturayı ya da seni s.... görüntüleri koyayım", "Nazillideyim gel görüşelim yoksa orayı başınıza yıkarım haber bekliyorum", "benim sana yaptığım masrafı yollamazsan 29 Nisan gecesi ..... Otelde kaldığımızı belgeleyen faturayı bütün Nazilli'ye, eşine, ailesine yollarım, kesinlikle haber bekliyorum en geç yarına" gibi mesajların içerikleri ve tüm dosya kapsamına göre, sanığın şantaj, bilişim sistemine girme ve özel hayatın gizliliğini ihlal suçlarını işlediği anlaşılmakla, TCK:nun 107/2, 243/1 ve 134/2. maddeleri uyarınca cezalandırılması gerekirken, yerinde olmayan gerekçelerle beraat hükümleri kurulması, (4. CD 18.03.2015, 2014/2222, 2015/24755)

30- Sanığın, katılan ile internette tanıştığı ve bir süre telefonda ve msn üzerinden görüntülü görüşerek arkadaşlık yürüttüğü, sanığın teklifi üzerine katılanın, kendisi, kızı ve sanık ile birilkte bir otelde yaklaşık 1 hafta süreyle tatil yaptıkları, arkadaşlıklarının bitmesi üzerine bilahare sanığın, katılanın kullandığı elektronik posta adresine rızası dışında birçok kez girdiği olayda, sanığın, bu şekildeki eyleminin TCK.nun 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturduğu ve mahkemenih hükmün gerekçesinde de eylem bu şekilde kabul edildiği halde, sanık hakkında

bilişim sistemine girme suçu yerine, TCK.nun 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan hüküm kurulmak suretiyle sanık hakkında fazla ceza tayini, (12. CD 13.01.2016, 2015/15933, 2016/277)

31- ... Bilişim sisteminde yapılan işlemler sonucu devamsızlık ve not düzeltmelerin dışında sağlandığı belirtilen haksız menfaatlerin ne olup kim tarafından sağlandığı karar yerinde açıklanıp tartışılmadan yetersiz gerekçe ile yazılı şekilde TCK.nun 244/4. maddesinin uygulanması (8. CD 15.02.2017, 2016/3794, 2017/1405)

32- ...TCK.nun 244/4. maddesindeki "yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde" şeklindeki düzenleme karşısında; şikayetçinin hesabına bilişim sistemi kullanılarak girmek sureti ile başka birinin hesabına şikayetçinin hesabından 4.985 TL havale etmek şeklindeki eylemin, TCK.nun 142/2-e madde ve fıkrasında yer alan nitelikli hırsızlık suçunu oluşturduğu gözetilmeden, TCK.nun 244/4. maddesi uyarınca mahkumiyet hükmü kurulması, (8. CD. 21.05.2018, 1115-5608)

KAYNAKLAR

Arslan, Prof. Dr. Çetin, Baştürk, İhsan, Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Veriler, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, cilt VIII, sayı:2, yıl:2013

Artuk, Prof. Dr. Mehmet Emin/Gökçen, Prof. Dr. Ahmet /Yenidünya, Doç. Dr. Caner Türk Ceza Kanunu Şerhi, Özel Hükümler, C. 5, Ankara 2009

Dülger, Doç. Dr. Murat Volkan, bilişim suçları ve internet iletişim hukuku, Ankara 2015, gül, G, ag

Efe, Dr. Ahmet, Bilişim Hukuku ile Uluslararası Hukuk Kesişiminde Yeni Bir Paradigma: Siber Yönetişim, Türkiye Noterler Birliği Hukuk Dergisi, Ankara, 2017, yıl:4 sayı:2

Erdoğan, Yavuz, Türk Ceza Kanununda bilişim sistemini engelleme bozma verileri yok etme değiştirme suçu, Doktora tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011

Gül, Ahmet, Doğrudan Dolaylı Bilişim Suçları, Seçkin, Ankara, 2019

Koca, Prof. Mahmut, Hukukumuzda TCK.nun 244. maddesi kapsamında bilişim sistemini engelleme, bozma verileri yok etme ve değiştirme suçu, bilişim hukuk konferansı, 9-10 Ekim 2008, Yargıtay Yayınları

Kurt, Levent, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınevi, Ankara 2005

Özgenç, Prof.Dr. İzzet, Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), Seçkin Yayınevi 2005

Taşdemir, Kubilay, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara 2009

Yargıtay Ceza Daireleri uygulamasında sıklıkla rastlanan bozma sebepleri, Yargıtay Cumhuriyet Başsavcılığı, Ankara 2018

Yaşar, Osman/Gökçen, Hasan Tahsin/Artuç, Mustafa, yorumlu uygulamalı Türk Ceza Kanunu, cilt V, Adalet Yayınları, Ankara 2010

YAZICIOĞLU, Yrd. Doç. Dr. R. Yılmaz, Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı, 21-22 Mayıs 2001, İzmir Uluslararası İnternet Hukuku Sempozyumunda sunulan tebliğ.