BİLİŞİM SİSTEMİNE GİRME SUÇUNUN YARGI KARARLARI BAĞLAMINDA İNCELENMESİ

THE CRIME OF UNAUTHORISED ACCESS TO COMPUTER SYSTEMS IN THE CONTEXT OF JUDICIARY DECISIONS

Hakemli Makale

Uğur İHTİYAROĞLU[*]

İÇİNDEKİLER

DOI: 10.32957/hacettepehdf.726568

Makalenin Geliş Tarihi: 25.04.2020 **Makalenin Kabul Tarihi:** 31.08.2020

[*] Cumhuriyet savcısı, Kırıkkale Üniversitesi Hukuk Fakültesi Kamu Hukuku Doktora Öğrencisi, E-posta: adaletbakanlik52@gmail.com

ORCID: 0000-0001-8171-3579

Çalışmada araştırma ve yayın etiği ilkelerine uyulmuştur.

ÖZ

Bilişim alanında 1990'lı yıllardan itibaren yaşanan gelişmeler bilgiye ve veriye ulaşma hızını hayal edilemeyecek derecede arttırmıştır. Bilişim teknolojileri insan hayatını kolaylaştırmakla birlikte toplumlar ve bireyler üzerinde tehlike oluşturabilecek bir silah haline de dönüşmüştür. Bilgisayar, cep telefonu ve internetin her alanda kullanımının yaygınlaşması, bu teknolojiler üzerinden suç işlenmesini kolaylaştırmaktadır. Bilişim suçlarının sürekli yaygınlaşması nedeniyle dijital sistemlerin ve verilerin korunması gerekliliği ortaya çıkmıştır. Bu nedenle bilişim sistemleri kullanımı yoluyla işlenen suçlar için ayrı düzenlemeler bulunması günümüz hukuk sistemleri açısından zorunludur. Bu çalışmanın amacı 5237 sayılı Türk Ceza Kanunu'nun (TCK) 243'üncü maddesinde yer alan "Bilişim Sistemine Girme" suçunu yargı kararları bağlamında incelemektedir. Türkiye'de bilişim sistemine girme suçunun yasal boyutu, ihlal koşulları, mukayeseli hukuk örnekleri, Bölge Adliye Mahkemeleri ve Yargıtay uygulamaları çalışmada analiz edilmiştir.

Anahtar Kelimeler: Bilişim teknolojileri, bilişim suçları, yargıtay kararları, dijital veri, internet

ABSTRACT

Developments in the field of informatics since the 1990s have increased the speed of access to information and data in an unimaginable way. While information technologies facilitate human life, it has also become a weapon that can pose a danger to communities and individuals. The widespread use of computers, mobile phones and the Internet in all areas makes it easier to commit crime through these technologies. The necessity of protecting digital systems and data has emerged due to the continuous spread of information technology crimes. Therefore, it is obligatory for today's legal systems to find separate regulations for crimes committed through the use of information systems. The aim of the study is to examine the crime of "Unauthorised Access to Computer Systems" in article 243 of the Turkish Criminal Law (TCK) numbered 5237 in the light of judicial decisions. The legal aspect of the crime of Unauthorised Access to Computer Systems in Turkey, violation conditions, comparative law examples, applications of Regional Courts of Justice and applications of Supreme Court were analyzed in the study.

Keywords: Information technologies, information crimes, supreme court decisions, digital data, internet

GİRİŞ

Bilişim sistemlerinin her dakika geliştiği bir zaman diliminde kişisel verilerin korunması, devlet ve ticaret sırrı olarak nitelendirilen gizli kayıtların dijital ortamda saklanması, bankaların müşterilerine ait hesapları kontrol altında tutması çok yönlü güvenlik tedbirlerini zorunlu kılmaktadır. Bu kapsamda dijital bilginin ve verinin korunması, günümüz hukuk sistemlerinin önemli öncelikleri arasında yer almaktadır.

Gelişen teknolojilerin insan hayatını kolaylaştırdığı 21'inci yüzyılda, yeni suç tiplerinin ortaya çıkması da muhtemeldir. Ceza hukuku alanında en hızlı değişim gösteren suç tiplerinin, bilişim suçları olduğunu söylemek mümkündür. Bu nedenle ulusal ve uluslararası mevzuatta bilişim sistemlerinin kullanılması yoluyla işlenen suçlar için ayrı düzenlemeler bulunmaktadır. 5237 sayılı Türk Ceza Kanunu'nun bilişim alanında suçlar bölümünde, hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu 243'üncü maddede düzenlenmiştir. Madde düzenlemesinde "*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. Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir. Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur. 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"* yer almaktadır. 5237 sayılı Türk Ceza Kanunu'nda 765 sayılı eski Türk Ceza Kanunu'ndan farklı olarak bilişim sistemlerinden bahsedilmiştir. Düzenleme incelediğinde, içeriğin daha çok engellemeye yönelik olduğu anlaşılmaktadır. Çünkü bilişim suçları genel olarak bir sisteme izinsiz olarak girilmesi sonucu ortaya çıkmakta ya da başlamaktadır. Düzenleme aşamasında maddenin gerekçesinde bilişim sistemlerinin "*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemler"* olarak açıklanması gelişen teknoloji nedeniyle birden fazla sistem aracılığıyla suçların işlenebileceğini ortaya koymaktadır. Sistemlerden kast edilen ise mekanik, elektronik ve manyetik araçlardır. Sadece bilgisayar, cep telefonu ve internet akla gelmemelidir. Birbirlerine bilişim ağı üzerinden

bağlanabilen her türlü sistem bilişim sistemi olarak nitelendirilebilir. Bilişim sistemine hukuka aykırı olarak erişim diğer suçların işlenmesine de imkân vereceğinden fiilin ayrıca cezalandırılması uygundur. Bilişim sistemine girme suçu, TCK 244 ve 245 ile birlikte doğrudan bilişim suçları içerisinde yer almaktadır. Bilişim sistemlerinin araç olarak kullanılması yoluyla işlenen suçlar ise genel olarak o suçla ilgili maddede düzenleme alanı bulmuştur. Örnek olarak TCK'nın 142'inci maddesinin 2'inci fıkrasının e bendinde yer alan nitelikli hırsızlık ve TCK'nın 158'inci maddesinin 1'inci fıkrasının f bendinde yer alan nitelikli dolandırıcılık suçları gösterilebilir.

Açıklananlar kapsamında bu çalışmada, bilişim sistemi kavramına değinilerek, bilişim sistemine girme suçunun elektronik ortamda hangi koşullar altında işlendiği, ihlal nedeniyle yerel mahkemeler tarafından verilen kararlar üzerinde Bölge Adliye Mahkemeleri ve Yargıtay tarafından yapılan incelemelerdeki tespitlerin neler olduğu ile uygulamada meydana gelen sorunlar ortaya konulmuştur.

I. SUÇUN KORUDUĞU HUKUKİ DEĞER

Bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme suçunda korunan birçok hukuki menfaat bulunmaktadır[1]. Ancak genel olarak TCK'nın 243'üncü madde düzenlemesi, bilişim suçları yönünden ilk basamak olarak nitelendirilmektedir. Diğer bilişim suçlarının işlenmesinde öncelikle bilişim sistemlerine girilmesi söz konusu olacağından, düzenleme engelleme amacını taşımaktadır. Bilişim sistemine girme suçunun yasal olarak mevzuatta yer alması;

- Toplum düzeninin korunması,
- Kişisel verilerin ve özel hayatın gizliliğinin korunması,
- Haberleşmenin gizliliğinin sağlanması,
- Kullanıcıların ve sistem üzerinde hak sahibi olanların korunması,
- Diğer bilişim yoluyla işlenen suçların engellenmesi,

[1] YENİDÜNYA, A. Caner, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu"**, Legal Fikri ve Sınai Haklar Dergisi**, Yıl:2005, Sayı:4, (s.1018-1042), s. 1024.

- Bilişim sistemlerinin ve programlarının güvenliğinin sağlanması amacına hizmet etmektedir. Ancak bu koruma özelinde doktrinde tartışma bulunmaktadır[2].

Bilişim sistemine girme suçunda, bilişim sisteminin dokunulmazlığı ön plandadır. 1990'lı yıllardan itibaren toplum hayatında internetin ve elektronik cihazların iletişimde büyük önem taşıdığı konusunda şüphe yoktur. Bilgisayarlar ve mobil cihazlar aracılığıyla saklanan kişisel verilerin korunması, bir bakıma özel hayatın gizliliği açısından da önem taşımaktadır. Bu durum Anayasa'nın 20'inci madde başlığındaki *"özel hayatın gizliliği"*[3] düzenlemesine de uygundur. Haberleşmenin ve iletişimin elektronik cihazlar üzerinden sağlanması ile bağlantıların gizliliğinin korunması ve istenmeyen kişiler tarafından ulaşımının engellenmesi bireysel özgürlüklerin konusu yapılmaktadır. Yetkisiz kişilerin iletişime dâhil olması düşünülemez. Düzenleme Anayasa'nın 22'inci maddesinde yer alan "*Haberleşme hürriyeti"*[4] ile doğrudan bağlantılıdır. Yetkisi olmayan kişilerin bilişim sistemine erişmesi ve bu sistem üzerinde hâkimiyet kurması, sistem sahiplerinin ve kullanıcıların mağdur olmasına yol açacaktır. Teknolojik gelişmelere bağlı olarak, bilişim sistemine girme suçu böylece diğer suçların işlenmesine olanak sağlamaktadır[5].

Ankara Bölge Adliye Mahkemesi bir kararında, *"Oluşa ve dosya kapsamına göre, katılan Ali'nin facebook adresinin şifresini bir şekilde ele geçiren sanığın, bu adresten katılan Ali gibi yazışarak, kendine haksız yarar sağlamak amacı ile Mazhar'dan para istemek şeklinde gerçekleştiği iddia olunan eyleminin, bilişim sistemine hukuka aykırı girmek suçu yanında TCK'nın 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu da 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*

---

[2] KARAGÜLMEZ, Ali, **Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri**, Seçkin Yayınevi, Ankara, 2009, s. 166.

[3] Anayasa madde 20/1: "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz*".

[4] Anayasa madde 22/1: "*Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır*".

[5] KETİZMEN, Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2008, s. 79.

verilmesi gerekirken, yargılamaya devamla yazılı biçimde hüküm kurulması" tespiti kapsamında bozma kararı vererek, failin müştekinin rızası dışında sosyal medya hesabına girmesini ve müştekiymiş gibi diğer şahıslarla yazışmasını bilişim sistemine girme suçu olarak nitelendirmiştir[6]. Suç yönünden sanığın, müştekinin sosyal medya hesabının şifresinin hangi şekilde ele geçirdiğinin önemi yoktur. Önemli olan bilişim sistemine hukuka aykırı olarak girilmesi veya orada kalınmasıdır. Benzer dosyada, *"...Bu açıklamalar ışığında incelenen dosya kapsamına göre, daha önce katılana ait eczanede çalışan sanıkların katılana ait medula şifresini onun bilgisi ve rızası dahilinde kullandıklarından şifreyi bildikleri, sanıkların katılana ait işyerinden ayrılıp .. Eczanesinde çalışmaya başlamalarından sonra bazı reçetelerde muayene katılım payı atlatma işlemi yapmak amacıyla katılana ait şifreyi kullanarak işlemleri gerçekleştirdikleri somut olayda, sanıkların eylemlerinin TCK'nın 243/1.maddesinde tanımlanan suçu oluşturduğu kabul edilmiş, meydana gelen zarar gözetilerek adli para cezası tercihle alt sınırdan uzaklaşılması, İlk Derece Mahkemesi kararı kaldırılarak aşağıda şekilde yeni bir hüküm kurulması gerektiği vicdani kanaatine varılmıştır"* şeklinde yapılan tespitler sonucu suçun bilişim sistemine girme olduğu, sanıkların katılanın şifresi ile hukuka aykırı olarak bilişim sistemine girerek atılı suçu işledikleri yönünde karar verilmiştir[7].

Bilişim sistemine girme, diğer suçların işlenmesine de hazırlık oluşturmaktadır. Yetkisiz girişlerin engellenmesinin bu açıdan önemi büyüktür. Bilişim sistemine girme suçu ile bilişim sisteminin bizatihi kendisinin koruma altına alınıp alınmadığı hususu ise doktrinde tartışmalıdır[8]. Bazı yazarlar hukuki korumadan bilişim sistemlerinin de yararlanmasının amaçlandığını kabul etmekle birlikte[9], bazı yazarlar ise bilişim sistemlerine dönük korumanın bulunmadığını ileri sürmektedir[10]. Ancak 2016 yılında

---

6 Ankara BAM 8. CD, 2019/704 E. 2019/267 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 20.03.2020)

7 Ankara BAM 12. CD, 2017/1339 E. 2018/871 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 25.03.2020)

8 TAŞKIN, Şaban Cankat, "Bilişim Hukuku Uluslararası Uyuşmazlıklar", **Türkiye Barolar Birliği Dergisi**, Yıl: 2009, Sayı:85, (s. 332-372), s. 335.

9 YAZICIOĞLU, Yılmaz, "Hackerler ve Bilişim Sistemine Girme Suçu", Ord.Prof. Dr. Sulhi Dönmezer Armağanı, Yıl: 2008, Cilt:1, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, **Atatürk Araştırma Merkezi ve Türk Ceza Hukuku Derneği Yayını**, (s. 1239-1261), s. 1254.

10 KARAGÜLMEZ, **2009**, s. 201

yapılan değişiklik sonucu, hukuka aykırı olarak sadece bilişim sisteminin tamamına veya bir kısmına girmenin veya orada kalmaya devam etmenin suç sayılması yani suçun seçimlik hareketli haline gelmesi nedeniyle bilişim sistemlerinin de koruma altında bulunduğunu söylemek mümkündür. 2016 yılı öncesinde, hem bilişim sistemine girme hem de orada kalmaya devam etme fiillerinin suçun oluşması açısından arandığından doktrinde tartışma yaşandığı anlaşılmaktadır. Suçun, kullanıcıların sanal ortamda rahatsız edilmemesi ve böylece kişisel hakların korunması amacıyla düzenlendiği yönünde görüşler bulunmakla birlikte[11], 243'üncü maddenin 2'inci fıkrasında fiil yönünden daha az cezayı gerektiren halin düzenlenmiş olması, mevzuat yönünden bilişim sisteminin korunmasının amaç edinilmediği görüşünü de ortaya çıkarmaktadır[12]. Bilişim sistemine girme suçu genel tabirle bireylerin dijital ortamdaki özel alanını koruma altına almaktadır. Madde gerekçesi hangi hukuki menfaate dönük olursa olsun, korunmak istenen sanal ortamdaki kişisel alan olarak ifade edilebilir[13].

II. SUÇUN UNSURLARI

Bilişim sistemine girme suçunun unsurları maddi unsurlar, manevi unsur, hukuka aykırılık unsuru, karşılaştırmalı hukuk ve suçun özel görünüş biçimleri olarak ayrı başlıklar halinde incelenecektir.

A. Suçun Maddi Unsurları

1. Fail

TCK'nın 243 madde metni incelendiğinde, suçta cezalandırılacak şahıs için 'kimse' tabiri kullanıldığı görülmektedir. Burada herhangi bir şart veya özellik aranmadığından, bu suçun faili herkes olabilir. Bilişim sistemine hukuka aykırı olarak giren veya orada kalmaya devam eden herkes bu suçun faili olacaktır. Sadece üstün bilgisayar becerisine sahip kişiler değil, aynı zamanda ortalama bilgisayar becerisine sahip kişiler de bu suçun

[11] KARAGÜLMEZ, **2009**, s. 201-202.

[12] APAYDIN, Cengiz, **Bilişim Suçları ve Bilişim Ceza Hukuku**, 1. Basım, Acar Matbaacılık, İstanbul, 2017, s. 51.

[13] KARAKEHYA, Hakan, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", **TBB Dergisi**, Yıl: 2009, Sayı:81, (s.1-24), s. 17.

faili olabilir[14]. Bu suçun failleri genel olarak bilişim korsanı, hacker veya craker olarak da isimlendirilmektedir[15]. Bilişim sistemine girme suçunun failinin tespit edilmesinde IP numarasının belirlenmesi önem taşımaktadır. Suçun failinin IP numarasının kayıtlı olduğu kişi olduğunun kabul edilmesi ile objektif sorumluluk esasına dayalı olarak yargılama yapılmaktadır. Ancak bu durumun Anayasa ve TCK yönünden hukuka aykırı olduğu ileri sürülmektedir[16]. Ankara Bölge Adliye Mahkemesi'nin bir kararında, "*Sanık hakkında TCK'nın 243 gereğince bilişim sistemine girme suçundan cezalandırılması istemi ile açılan kamu davasında, kolluk görevlileri yapılan .....A.Ş kayıtlarında sanığın, Bayram'ın babası Osman'ın IP numarasının tespit edildiği, sanığın babasının bilgisayarın oğlu Bayram tarafından kullanıldığını beyan ettiği, sanığın atılı suçu işlediği yönünde aşamalarda hiç bir ikrarının bulunmadığı, IP adresinin iddianamede delil olarak gösterildiği ancak IP adresinin kişiye özel olmadığı, IP'nin teknik açıdan değiştirilebilir yapıda olduğu, başka bir kişinin de mevcut IP adresini kullanabileceği, sistem havuzunda IP adresinden çıkıldıktan sonra başkasının da IP'yi kullanabileceği, internet üzerinden alışverişin herhangi bir kişi tarafından da yapılabileceği, abonelik üzerinden başkalarının da bağlanmış olabileceği göz önüne alınarak bu hususların açıklığa kavuşturulması amacıyla bilirkişi raporu alınmaksızın eksik inceleme ile yazılı şekilde karar verilmesi"* bozma nedeni olarak yer almakla, bilişim sistemine girme suçunun oluşması için gerekli tüm tespitlerin yapılmasının zorunlu olduğu, somut olayın niteliğine göre bilirkişi raporu alınmadan dosya üzerinden karar verilemeyeceği ortaya konulmuştur[17]. Özellikle IP adresinin değiştirilebilir nitelikte olduğu ve birçok kişi tarafından kullanılabileceği dikkate alınarak inceleme yapılması, teknik olarak failin tespitinin kuşkuya yer vermeyecek şekilde belirlenmesi kararda vurgulanmıştır. Yargıtay'ın bir ilamında, "*Bilişim sistemine girmek, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla*

---

[14] YENİDÜNYA, A. Caner/DEĞİRMENCİ, Olgun, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, 1. Basım, Legal Yayıncılık, İstanbul, 2003, s. 57.

[15] ERDOĞAN, Yavuz, "Bilişim Sistemine Girme ve Kalma Suçu", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Yıl:2010, Cilt: 12, Özel Sayı, (s.1363-1433), s. 1392.

[16] APAYDIN, **2017**, s.53.

[17] Ankara BAM 13. CD, 2018/3653 E. 2019/1533 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 20.03.2020)

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. Somut olayda; 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 sorulması gerektiği gözetilmeden eksik inceleme ile hüküm kurulması" bozma nedeni olarak kabul edilmiştir[18]. Kararda, fail tarafından gerçekleştirilen bilişim sistemine girme eyleminin şüpheye yer bırakmayacak şekilde araştırılması gerektiği, özellikle IP numarası üzerinde kuşkuya yer vermeyecek şekilde inceleme yapılarak sonucuna göre karar verilmesi hususu ortaya konulmuştur.

2. Mağdur

Suçun mağduru, bilişim sistemine girilen ve bu nedenle kişisel hakları tehlikeye düşen kişidir. Doktrinde suçun mağdurunun gerçek kişiler dışında, tüzel kişiler de olabileceği ileri sürülmektedir. Suçla korunmak istenen bilişim sisteminin güvenliği olduğundan, bilişim sistemlerinin sahiplerinin tüzel kişiler olması durumunda tüzel kişilerin mağdur olması mümkün olacaktır[19]. Ancak bazı araştırmacılar tüzel kişilerin

[18] Yargıtay 8. CD, 2018/1078 E. 2018/2485 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 20.03.2020)

[19] ERDOĞAN, **2010**, s.1394.

suçun mağduru olamayacağını yalnızca suçtan zarar gören olabileceğini kabul etmektedir[20]. Bizim görüşümüz de tüzel kişilerin mağdur olabileceği yönündedir. Çünkü bilişim sistemi üzerinde hak sahibi olan herkes suçun mağduru olabilir. Bilişim sistemi üzerinde hak sahibi olmak, mülkiyet hakkı sahibi olmakla gerçekleşebileceği gibi kira, ariyet gibi sözleşmelerden de doğabilir. Bu nedenle tüzel kişilerin de bilişim sistemi ve/veya veriler üzerinde tasarruf yetkisi bulunması söz konusudur[21]. Fail tarafından gerçekleştirilen eylemin birden fazla kişinin hakkını ihlal etmesi durumunda; bu şahısların tamamının suçun mağduru olacağı ileri sürülmektedir. Örneğin, bilişim sisteminde üçüncü şahıslara ait verilerin bulunması durumunda hem bilişim sisteminin sahibinin hem de verilerin sahibinin suçun mağduru olacağı savunulmaktadır. Ancak suç konusu fiil, bilişim sistemi üzerinde gerçekleşmektedir. Bu nedenle bilişim sistemi içinde yer alan dijital kayıtların ve verilerin kime ait olduğu konusu suç yönünden önemli değildir. Veriler suçun konusu olamayacağı için incelemede dikkate alınamaz. Veriler yönünden TCK. 136 maddesinde yer alan suç değerlendirilmelidir[22]. Siber suçların yapısı gereği sürekli yaygınlaşmaktadır. Bu nedenle suçlar, bireylere ve tüzel kişilere karşı işlenebileceği gibi hükümete karşı da işlenebilir[23].

3. Suçun Konusu

Bilişim sistemine girme suçunun konusu bakımından öncelikle bilişim ve bilişim sistemi kavramlarının açıklanması gereklidir. Dünyanın birçok ülkesinde belgeleme ve veri elde etme tekniğinin gelişimi ile birlikte bilişim ayrı bir disiplin sistemi olarak algılanmaya başlamıştır. Bilişim kavramı, insanların gündelik yaşantılarında sahip oldukları teknik, ekonomik, sosyal, mali, kültürel ve hukuki verilerinin saklanması, saklanan bu verilerin gerektiğinde işlenmesi, bilişim ağları ve iletişim araçları yoluyla

---

[20] MAHMUTOĞLU, Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Yıl:2013, Cilt: 71, Sayı: 1, (s. 855-889), s. 860-861.

[21] KURT, Levent, **Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanununda Uygulaması**, Seçkin Yayınevi, Ankara, 2005, s. 163.

[22] ERDOĞAN, **2010**, s.1394-1395, TCK. madde 136: Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

[23] TRIPATHI, Esha/ TRIPATHI, Abhay/YADAY, Mithilesh Kumar Singh, "Role of Information Technology in Cyber Crime and Ethical Issues in Cyber Ethics", **International Journal of Business and Research (IJBER)**, Yıl: 2016, Cilt: 10, (s. 1-5), s. 2.

aktarılması olarak açıklanmaktadır[24]. Telekomünikasyon ve bilgi işlem teknolojilerinde yaşanan hızlı ilerleme bugün anında veri alma ve iletmeye imkân sağlamaktadır. Bilgisayar, mobil cihazlar ve diğer kitle iletişim araçları üzerinden sesli, yazılı ve görüntülü içerikler paylaşılmakta; kablosuz teknolojiler gün geçtikte yaygınlaşmaktadır[25]. 765 sayılı Türk Ceza Kanunu düzenlemesinde bulunan *"bilgileri otomatik olarak işleme tabi tutmuş sistem"* yerine 5237 sayılı Türk Ceza Kanunu'nda *"bilişim sistemi"* tabiri kullanılmıştır. Bilişim teknolojilerinin hızla gelişmesi, elektronik aletlerinin boyutlarını küçültmüş; kullanıcı sayısında büyük artışlar yaşanmıştır[26].

Türk Ceza Kanunu düzenlemesi kapsamında bir sistemin bilişim sistemi olup olmadığını tespit etmek teknik bir konudur ve somut olayın niteliğine göre uzman kişiler tarafından tespit edilmelidir. Bu nedenle kavramların doktrin açısından neler ifade ettiği açıklanmalıdır[27]. Bilişim ve bilişim sistemi kavramları, bilgisayar ve internet gibi kavramlarla doğrudan ilişkilidir. Özellikle 1990'lı yıllardan sonra insanların bilgiyi depolama, paylaşma ve bilgiye hızlı şekilde ulaşma isteği sonucu yaygınlaşan internet, bilgisayar sistemlerini birbirlerine bağlamış; küresel boyutta iletişim ağı oluşturmuştur. Farklı bilgisayarların ortak bir alan içerisinde birbirlerine bağlanması sonucu oluşan elektronik ağ (Network) meydana gelmiştir. Artık bilgisayar, cep telefonu, tablet gibi elektronik cihazların bu ağlara katılmasıyla milyarlarca insan çevrimiçi olarak bilgi alışverişinde bulunmaktadır[28]. Ancak bilişim ve bilişim sistemlerinin tanımlanması için sadece internet ve bilgisayar üzerinden açıklama yapılması yeterli değildir. Çünkü bilgisayar dışında da verileri otomatik olarak işleyen ve veriler arasında bağlantı sağlayabilen elektronik ve manyetik cihazlar bulunmaktadır. Bu cihazlar bağlantıyı soyut

---

[24] ERDAĞ, Ali İhsan, "Bilişim Alanında Suçlar (Türk ve Alman Hukukunda)", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Yıl:2010, Cilt:14, Sayı: 2, (s.275-303), s. 277.

[25] ATASOY, Fahri, "Kültürler Üzerinde Bilişim Devriminin Etkileri", **Modern Türklük Araştırmaları Dergisi**, Yıl: 2007, Cilt: 4, Sayı: 2, (s.163-178), s. 166.

[26] KOÇAK, Hüseyin/DANDİN, Ali Nazmi, "Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri", **Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi**, Yıl:2017, Cilt: 19, Sayı: 1, (s. 137-152), s. 139-140.

[27] APİŞ, Özge, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri", **Yasama Dergisi**, Yıl: 2018, Sayı: 37, (s. 49-86), s. 55.

[28] TEKELİ, Ömer, "Bilişim Suçlarıyla Mücadelede Polisin Yeri", **Sayder Dış Denetim Dergisi**, Sayı:2011 Temmuz-Ağustos-Eylül, (s.183-192), s. 184.

ve somut olarak sağlayarak veri akışını gerçekleştirmektedir. Örneğin, internet ağı kullanılmaksızın manuel olarak ya da intranet üzerinden de suç işlenebilir[29]. 5237 sayılı Türk Ceza Kanunu yönünden bilişim sistemine girme suçunun işlenebilmesi için, somut olayda sistemin bir bilişim sistemi olarak tanımlanması zorunluluğu bulunmaktadır. Bilişim sistemine hukuka aykırı olarak girilmesi veya hukuka aykırı olarak orada kalmaya devam edilmesi suçun temel şeklini oluşturmaktadır. Bilgisayar veri sistemine izinsiz şekilde giriş yapan kişiler "bilgisayar korsanı" veya "hacker" olarak tanımlanmaktadır. Hukuk doktrininde bilişim sistemine girme suçunda *"girme"* yerine *"erişim"* kavramının kullanılmasının yerinde olup olmadığı tartışılmaktadır. Bunun nedeni ise suçun sanal ortamda gerçekleşmesi yani somut bir fiilin bulunmamasıdır[30]. Bilişim sistemi ayrıca 243'üncü maddenin gerekçesinde de açıklanmıştır. Bu açıklama kapsamında, bilişim sistemi "*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tutma olanağı veren manyetik sistemler*" olarak tarif edilmiştir. Diğer yandan bilişim sistemleri verileri toplama, işleme, çoğaltma, değerlendirme gibi çok yönlü olarak otomatik işlemlere tabi tutma imkânı sağlayan sistemler olarak da kabul edilmektedir[31]. Avrupa Konseyi Siber Suçlar Sözleşmesinin 1. maddesinde "bilgisayar sistemi" ifadesine yer verilmekle birlikte bu kavram yönünden "*bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder*" şeklinde tanım getirilmiştir. Türkiye bu sözleşmeye taraf olmakla birlikte, bilişim suçları yönünden "bilgisayar suçu" veya "bilgisayar aracılığıyla işlenen suç" terimlerinin kullanılması sıklıkla eleştirilmektedir[32]. Yargıtay Ceza Genel Kurulu tarafından verilen bir kararda *"elektronik beyin" veya "bilgileri otomatik işleme tabi tutmuş sistem" olarak adlandırılan bilgisayar; "çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran, bilgileri depolayan elektronik araç, elektronik beyin" anlamına gelmektedir. İnternet ise, dünya üzerindeki*

---

[29] BOSS, Richard W, "Intranet and Extranet", **PLA Tech Notes, American Library Association**, Yıl: 2010, (s.1-4), s. 3.

[30] KARAGÜLMEZ, **2009**, s. 169.

[31] KOCA, Mahmut/ÜZÜLMEZ, İlhan, **Türk Ceza Hukuku Özel Hükümler**, 4. Basım, Adalet Yayınevi, Ankara, 2017, s. 810.

[32] YENİDÜNYA/DEĞİRMENCİ, **2003**, s.27.

milyonlarca bilgisayarın birbirlerine bağlanmaları ile oluşan global bir bilgisayar ağları sistemini ifade eder. Bilişim de; "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi" olarak tanımlanmaktadır. Yerleşmiş yargısal kararlar ve öğretideki baskın görüşlere göre de, bilişim sisteminin, verileri toplanıp yerleştirdikten sonra otomatik işleme tabi tutma imkânı veren manyetik sistemler olduğu kabul edilmiştir" yer almaktadır[33].

Bu açıklamalar ışığında bilişim sistemine girme suçunun konusunu, tamamına veya bir kısmına hukuka aykırı olarak girilen veya içerisinde kalınan bilişim sistemi oluşturmaktadır. TCK'nın 243'üncü maddesinin 2'inci fıkrası yönünden suçun konusunu "*bedeli karşılığında yararlanılabilen bilişim sistemleri*" oluşturmaktadır. Eğer suçun konusu "*Otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmet*" ise, TCK'nın 163'üncü maddesinde yer alan "*Karşılıksız Yararlanma*" suçu meydana gelecektir[34]. Bu fıkranın somut olaya uygulanabilmesi için bilişim sisteminin bedel karşılığı yararlanılabilen bir sistem olması gerekmektedir. Fail tarafından bedeli ödenmek suretiyle girilebilecek bir sisteme, bedel ödenmeden girilmesi veya orada kalınması gereklidir. Bedel karşılığı yararlanılabilen bilişim sistemlerinin neler olduğu konusu madde gerekçesinde açıklanmamıştır. Ancak bu sistemlerden genel olarak anlaşılan, internet üzerinden hizmet veren web siteleri, kiralama karşılığı yararlanılabilen bilişim sistemleri, cep telefonları ve diğer elektronik cihazlara anlaşma karşılığı gönderilen reklam mesajları ve mailler, internet servis sağlayıcı hizmetlerinden yararlanılması uygulamaları anlaşılmaktadır[35].

Kanun koyucu TCK'nın 234'üncü maddesinin 3'üncü fıkrasında suçun neticesi sebebiyle ağırlaşmış halini düzenlemiştir. Doktrinde bu düzenlemeyi bağımsız bir suç

---

[33] Yargıtay Ceza Genel Kurulu, 2016/23-1033 E. 2020/2 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 20.08.2020)

[34] YILMAZ, Zahit/ APİŞ, Özge, "Karşılıksız Yararlanma Suçu (TCK m.163)", **MÜHFHAD**, Yıl: 2013, Cilt: 19, Sayı: 2, (s.1749-1779), s. 1767.

[35] ERDOĞAN, **2010**, s.1396-1399.

olarak değerlendiren görüşler de bulunmaktadır[36]. Bu görüşte olanlar, suçun ayrı bir fıkra olarak düzenlenmesi ve temel şekle nazaran taksire dayalı sorumluluğu içermesi nedenlerini ileri sürmektedir. Ancak çoğunluk tarafından kabul edilen ve bizim de katıldığımız görüş, verilerin yok olması veya değiştirilmesinin bilişim sistemine girme suçunun neticesi sebebiyle ağırlaşmış hali olduğudur[37]. Bilişim sistemine hukuka aykırı olarak girilmesi veya orada kalmaya devam edilmesi durumunda "*sistemin içerdiği veriler yok olur veya değişirse*" failin cezası artacaktır. Bu fıkranın uygulama alanı bulabilmesi için TCK'nın 23'üncü maddesinde yer alan koşulların somut olayda meydana gelmesi gereklidir. Failin temel kastının sadece bilişim sistemine hukuka aykırı girme veya orada kalma olması zorunludur. Failin sistemdeki verileri yok etme veya değiştirmeye yönelik bir kastı olmamalıdır. Ancak failin kastı bulunmasa da bilişim sistemine hukuka aykırı erişim sonucu veriler yok olur veya değişirse; failin söz konusu bu ağırlatıcı sebepten sorumlu tutulabilmesi için kastını aşan neticeye yönelik en azından taksirinin bulunması gerekir. Burada TCK'nın 244'üncü maddesinde yer alan "*Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme*" suçundan farklı olarak failin sisteme hukuka aykırı olarak girmesi veya orada kalması durumunda sistemdeki veriler yok olmakta veya değişmektedir. Verilerin yok olması veya değişmesi durumunda failin kastının söz konusu olduğu hallerde TCK'nın 244'üncü maddesinin 2'inci fıkrası uygulama alanı bulacaktır. Bir bakıma suçun taksirli hali TCK'nın 243'üncü maddesinin 3'üncü fıkrasında düzenleme alanı bulmuştur[38]. Failin hukuka aykırı olarak bilişim sistemine girme veya orada kalma kastının bulunmaması durumunda suçun temel şekli meydana gelmeyeceğinden failin sorumluluğu doğmayacaktır. Bu halde TCK'nın 243'üncü maddesinin 3'üncü fıkrası oluşmayacağı gibi ancak kasten işlenebilen TCK'nın 244'üncü maddesinin 2'inci fıkrasının uygulanması söz konusu olamaz[39]. TCK'nın

---

[36] MALKOÇ, İsmail, **Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu**, Malkoç Kitabevi, Cilt: 2, Ankara, 2007, s. 1671; EKER, Ö. Umut, "Türk Ceza Hukuku'nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 s. Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", **Türkiye Barolar Birliği**, Yıl: 2006, Sayı: 62, (s. 123-131), s. 124.

[37] ÖZBEK, Veli Özer / DOĞAN, Koray/BACAKSIZ, Pınar/TEPE, İlker, **Türk Ceza Hukuku Özel Hükümler**, 11. Basım, Seçkin Yayınevi, Ankara, 2017, s. 951.

[38] YAZICIOĞLU, Yılmaz, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi", **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Yıl: 2005, Cilt: 2, Sayı: 2, (s. 401-409), s. 403.

[39] APAYDIN, **2017**, s. 71.

243'üncü maddesinin 4'üncü fıkrası yönünden ise suçun konusunu *"Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakilleri"* oluşturmaktadır.

İstanbul Bölge Adliye Mahkemesi tarafından verilen bir kararda *"Dosya kapsamından sanığın, eşi olan müştekinin telefonunda kayıtlı müştekiye ait çıplak fotoğrafları, yine müştekinin telefonunda bulunan Whatsapp hesabına rızası olmadan girerek bu hesaptan müştekinin ailesine göndermek suretiyle paylaşması şeklinde gerçekleşen eyleminin bir bütün olarak TCK'nın 244/2. maddesinde düzenlenen suçu oluşturacağı anlaşılmakta ise de, istinaf kanun yoluna sanığın gelmiş olması dikkate alınarak aleyhe istinaf olmadığından bu husus eleştirilmekle yetinilmiştir"* yer almaktadır[40]. Dosya kapsamında sanık, müştekinin telefonuna rızası dışında girmiş ve telefonda yer alan verileri paylaşmıştır. Bu nedenle suçun bilişim sistemine girme değil, TCK'nın 244'üncü maddesinin 2'inci fıkrası kapsamında *"var olan verilerin başka bir yere gönderilmesi"* olduğu tespit edilmiştir. Somut olayda verilerin başka bir yere gönderildiği, bir bakıma bilişim sistemine girme suçunun TCK'nın 244'üncü maddesinin 2'inci fıkrası kapsamına dâhil olduğu kabul edilmiştir. Diğer taraftan failin var olan verileri paylaşması kapsamında suçun artık TCK'nın 243'üncü maddesi kapsamında değerlendirilemeyeceği anlaşılmıştır. Kişisel verilere yetkisiz şahısların erişimi bu suçun konusunu oluşturmaktadır[41]**.** Yargıtay'ın bir kararında *" Sanığın, eski eşi olan mağdura ait facebook şifresini bildiğini ve şifre kırma gibi bir eyleminin olmadığını beyan etmesi, mağdurun, şifresinin kırılarak facebook hesabına giriş yapıldığına dair iddialarını doğrulayan herhangi bir delil bulunmaması karşısında, sanığın sübut bulan bilişim sistemindeki mağdura özel kısma girip, hakkı olmadığı halde sistemde kalmaya devam etme eyleminin TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme ve mağdura ait içeriği özel mesajları okuyup, tarafı olmadığı haberleşme içeriklerini kaydetmesi eyleminin TCK'nın 132/1. madde ve fıkrasındaki haberleşmenin gizliliğini ihlal suçlarını oluşturacağı gözetilmeden, delillerin takdirinde ve suç vasfında yanılgıya düşülerek, sanık hakkında TCK'nın 244/2. madde ve fıkrasındaki sistemi engelleme, bozma, verileri*

[40] İstanbul BAM 17. CD, 2018/3376 E. 2019/896 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 25.03.2020)

[41] ERDOĞAN, **2010**, s.1398-1399.

yok etme veya değiştirme ve TCK'nın 136/1. madde ve fıkrasındaki verileri hukuka aykırı olarak verme veya ele geçirme suçlarından mahkûmiyet kararı verilmesi" bozma nedeni yapılmıştır[42]. Failin bilişim sistemine girmesi ancak şifre değiştirme veya kırma gibi bir eyleminin bulunmaması karşısında suçun TCK'nın 244'üncü maddesinde yer alan suçu değil, bilişim sistemine girme suçunu oluşturacağı vurgulanmıştır. Failin fiilinin, TCK'da yer alan diğer suçları da oluşturması durumunda somut olaya göre inceleme yapılması gerekecektir. Benzer dosyada "*Sanıkların …… Esnaf ve sanatkarlar odası üyelerine ait ellerindeki bilgilerin doğruluğunu teyit etmek için Nüfus ve Vatandaşlık İşler Genel Müdürlüğü ile anlaşma yapıp ücreti karşılığı yararlanmak yerine bir yazılım ile müşteki şirketin bilişim sistemine veri gönderip, seri şekilde milyonlarca sorgu yapıp sistemde var olan verileri aldıkları anlaşıldığından sanıkların eyleminin 5237 sayılı TCK'nun 244/2-4 maddelerinde düzenlenen suçu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemine girme suçundan mahkumiyetlerine karar verilmesi*" bozma nedeni yapılmıştır[43]. Somut olayda failin kastının tespit edilmesi ile meydana gelen sonuç arasındaki ilişki suç tipinin tespit edilmesinde önem taşımaktadır. Yargıtay'ın bir kararında "*Sanık hakkında bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan verilen hüküm açısından; dosya kapsamına göre sanığın, katılan Meltem'in elektronik posta adresinin ve facebook hesabının şifrelerini kırarak, hesaba giriş şifresini değiştirerek erişimini engellemesi şeklinde gerçekleşen eyleminin TCK'nın 244/2. maddesi kapsamında kaldığı halde suç vasfında hataya düşülerek aynı yasanın 243/1. maddesinden mahkûmiyet hükmü kurulması"* bozma nedeni yapılmıştır[44]. Yargılama aşamasında failin kastının, TCK 243 ve 244 yönünden ayrı ayrı değerlendirilmesi gerektiği kararda vurgulanmıştır.

4. Fiil (Hareket)

TCK'nın 243'üncü maddesinin ilk fıkrasında suçu oluşturan fiil, bir bilişim sisteminin bütününe veya bir kısmına "*hukuka aykırı şekilde girme*" veya "*orada kalmaya devam etme*" olarak düzenlenmiştir. 6698 Sayılı Kanun'un 30'uncu maddesi kapsamında

[42] Yargıtay 12. CD, 2019/577 E. 2019/12248 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 21.08.2020)

[43] Yargıtay 15. CD, 2017/14178 E. 2020/4067 K. (Uyap Bilişim Sistemi, Erişim Tarihi 20.08.2020)

[44] Yargıtay 15. CD, 2017/30133 E. 2018/2657 K. (Uyap Bilişim Sistemi, Erişim Tarihi 20.08.2020)

yapılan değişiklikle birlikte fıkrada yer alan 've' ibaresi 'veya' şeklinde değiştirilmiştir. Geçmişte suçun oluşumu için bir bilişim sisteminin tamamına veya bir kısmına girmek yeterli olmayıp, belirli bir süre sistemde kalınması da gerekmekteyken[45], artık sisteme hukuka aykırı olarak girilmesi veya orada kalınması suçun oluşumu için yeterli olmuştur. TCK'nın 243'üncü maddesinin 2'inci fıkrası yönünden "*hukuka aykırı şekilde girme*" veya "*orada kalmaya devam etme*" fiillerinin "*bedeli karşılığında yararlanılabilen bilişim sistemleri*" üzerinde gerçekleştirilmesi zorunludur. Dijital dünyada ve iş yaşamında bu suç daha çok şirket sırlarının ve yazışmaların korunması amacına dönüktür. Ancak ticari kurum ve kuruluşların haklarının güvence altına alınması amacıyla özgülenen madde cezada indirim öngörmesi nedeniyle bir bakıma failleri suç işlemeye teşvik etmektedir. Sistemde kalma fiilinin bir müddet devam etmesi zorunludur. Ancak sürenin yeterliliği mahkemelere bırakılmıştır. Bu nedenle hukuk alanında görev yapanların bilişim alanında sahip olduğu bilgilerin önemi büyüktür. Suçun oluşumu yönünden, yargılama aşamasında bilişim alanında bilgi sahibi bir fail ile acemi ve bilgisi yetersiz bir failin kıyaslamasının yapılması gerekecektir[46]. Suçun temadi eden niteliği de yargılama sürecinde dikkate alınacaktır.

Fail sisteme zaman zaman girip çıkıyorsa her giriş çıkış nedeniyle ayrı ayrı cezaya hükmedilmeyecek, zincirleme suç hükümleri göz önünde tutulacaktır[47]. TCK'nın 243'üncü maddesinin 3'üncü fıkrası bakımından "*hukuka aykırı şekilde girme*" veya "*orada kalmaya devam etme*" sonucu sistemin içerdiği verilerin yok olması veya değişmesi gereklidir. TCK'nın 243'üncü maddesinin 4'üncü fıkrası bakımından ise "*veri nakillerinin sisteme girmeksizin teknik araçlarla hukuka aykırı izlenmesi"* suçun oluşumu için zorunludur.

Bilişim sistemine hukuka aykırı olarak girilmesi, fiziki olarak yapılan bir müdahaleyi ifade etmemektedir. Burada ifade edilen bir bilişim sisteminin tamamına ya

---

45 MAHMUTOĞLU, **2013**, s. 860.

46 GÖNEN, Serkan/ULUS, Halil İbrahim/ YILMAZ, Ercan Nurcan, Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, **Bilişim Teknolojileri Dergisi**, Yıl: 2016, Cilt:9, Sayı:3, (s. 229-236), s. 230.

47 AVŞAR, B. Zakir/ÖNGÖREN, Gürsel, Bilişim Hukuku, **Türkiye Bankalar Birliği**, Yıl:2010, Yayın No: 270, (s.1-344), s. 134.

da bir kısmına hukuka aykırı olarak erişmek, ulaşmaktır[48]. Örneğin, bilgisayarın kasasının açılarak içine girilmesi, bilgisayar parçalarına zarar verilmesi, bu suçu oluşturmayacaktır; şartlarının bulunması durumunda 'mala zarar verme' suçu oluşabilecektir[49]. Bilişim sistemine girilmesi, açık olan bir bilgisayardan verilere ulaşılması yoluyla olabileceği gibi; ağlar ve internet üzerinden de gerçekleşebilir. Suçun meydana gelmesinde, bağlantının kablolu, kablosuz olması; mesafenin uzak veya yakın olmasının bir önemi yoktur. Bir sisteme sadece e-posta gönderilmesi ve gönderilen dosyanın içinde yer alan programın sisteme girme imkânı vermemesi durumunda bilişim sistemine girme suçundan söz edilemez. Ancak program aracılığıyla sisteme giriş yapma imkânı varsa suç oluşabilir. Gönderilen e-postanın açılmaması durumunda ise teşebbüsten bahsedilebilir. 2016 yılında 6698 Sayılı Kanunla yapılan değişiklik sonucunda suç, seçimlik hareketli hale gelmiştir. Suçun meydana gelmesi için sisteme girmek yeterli kabul edilmekte ayrıca sistemde kalma aranmamaktadır. Sistemde kalmaya devam etme ifadesi suç yönünden daha uzun bir temadiyi oluşturmaktadır. Kanun koyucu burada sistemde 'kalan' ifadesi yerine sistemde 'kalmaya devam eden' ifadesini kullanmıştır. Bilişim sistemlerinin özelliği ve somut olaya göre sistemde kalmaya devam etme olgusunun değerlendirilmesi gereklidir. Bu nedenle kalmaya devam etme fiilinin süresi açısından bir kesinlik yoktur. Bazı yazarlar süre yönünden, failin başkasının bilişim sistemine hukuka aykırı olarak girdiğini fark etmesi/girmesi durumunda yeterli sürede o sistemden uzaklaşıp uzaklaşmadığının değerlendirilmesi gerektiğini ileri sürmektedir[50]. Fail tarafından bilişim sistemine girilip hiçbir işlem yapılmaksızın sistemden çıkılsa dahi suç meydana gelmiş olacaktır. Suç bu yönüyle tehlike suçu olarak kabul edilmektedir[51]. Suçu doktrinde yetkisiz erişim olarak kabul eden yazarlar da bulunmaktadır[52]. Yargıtay'ın bir ilamında, "*Bilişim sistemine girme ve engelleme suçundan verilen beraat hükmüne yönelik o yer Cumhuriyet Savcısının temyiz talebinin incelenmesinde, sanığın katılanın hesaplarının*

48 MAHMUTOĞLU, **2013**, s. 860.

49 TAŞKIN, Şaban Cankat, **Bilişim Suçları**, 1. Basım, Beta Yayınları, İstanbul, 2008, s. 25.

50 MAHMUTOĞLU, **2013**, s. 861.

51 MAHMUTOĞLU, **2013**, s. 862.

52 TEZCAN, Durmuş/ERDEM, Mustafa Ruhan/ ÖNOK, R. Murat, **Teorik ve Pratik Ceza Özel Hukuku**, Seçkin Yayınevi, Ankara, 2018, s. 1036, KETİZMEN, **2008**, s.100.

şifresini ele geçirip, ardından şifreleri değiştirmesi şeklindeki eylemi ile şikâyetçiden para istemesi eyleminin iki ayrı suçu oluşturması karşısında; TCK'nın 44. maddesinin uygulanma imkânının bulunmadığı, ayrıca iddia makamının talep ettiği kanun maddesinin sanık için kazanılmış hak oluşturmayacağı da göz önüne alındığında, tebliğnamedeki TCK'nın 243/1 maddesi gereğince bozma isteyen düşünceye iştirak edilmemiş olup, sanığın katılanın posta adresinin ve facebook hesabının şifresini kırması, ardından da şifreyi değiştirmesi şeklindeki eyleminden dolayı TCK'nın 244/2 maddesinde düzenlenen bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, sisteme veri yerleştirme suçundan da mahkûmiyet kararı verilmesi gerekirken yazılı şekilde hüküm kurulması" bozma nedeni yapılmıştır[53]. Kararda bilişim sistemine girme suçu yanında ayrıca TCK'nın 244'üncü maddesinin 2'inci fıkrası uyarınca mahkûmiyet hükmü kurulabileceği belirtilmiştir. O halde somut olaya göre tespit yapılarak failin fiili değerlendirilmeli, sonucuna göre suç tipi ortaya konulmalıdır. Benzer dosyada *"Katılanın e-mail ve facebook hesabına izinsiz girip hesapların şifrelerini değiştirmek suretiyle bilişim sistemine girmesini engellediğinden bahisle açılan davada; bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme ile bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, var olan verileri başka bir yere gönderme suçlarında, gerçekleşen eylemlerin bir bütün olarak TCK.'nın 244/2. maddesinde düzenlenen suçu oluşturacağı, katılanın hesabına giriş yaptığına ilişkin sanığın bu hesaba ait e-mail şifresinin değiştirildiğine dair dosya içerisinde bir tespitin bulunmaması ancak katılanın hesabına girişinin engellediğini iddia etmesi karşısında, suç tarihinden şikâyet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, şikâyetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı, sanık tarafından adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığı ilgili internet sağlayıcısından sorulup, sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmaya dayanarak ve eylem ikiye bölünerek yazılı şekilde ayrı ayrı hükümler kurulması"* bozma nedeni yapılmıştır. Sanık üzerine atılı suçun katılanın sosyal medya hesabı ile e-mail şifrelerini rızası dışında değiştirme olduğu ancak suçun fail

[53] Yargıtay 15. CD, 2017/31912 E. 2018/2652 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 25.03.2020)

tarafından gerçekleştirildiği yolunda kesin kanaatin oluşmadığı, dosya kapsamında araştırılması gereken hususların ayrı ayrı incelenmesi gerektiği belirtilmiştir[54]. Diğer taraftan iddia konusu suçun müştekiye ait hesabın şifrelerinin değiştirilmesi olduğundan, yargılamanın TCK'nın 243'üncü kapsamında bilişim sistemine girme suçundan değil, TCK'nın 244'üncü maddesinin 2'inci fıkrasında düzenlenen suçtan yapılması gerektiği vurgulanmıştır.

5. Netice

TCK'nın 243'üncü maddesinde yer alan bilişim sistemine girme suçunun oluşması için hukuka aykırı olarak bir bilişim sisteminin bütününe veya bir kısmına girilmesi veya orada kalınması gereklidir. 6698 Sayılı Kanunun 30'uncu maddesi ile yapılan düzenleme sonucu suç çok hareketli iken, seçimlik hareketli hale gelmiştir. Yapılan değişiklikle, herhangi bir kasıt olmaksızın başkasının bilişim sistemine girilmesi ile oluşan hukuka aykırılığın fark edilmesi ancak sistemde kalınmaya devam edilmesi de suç kapsamına alınmıştır[55]. Girme veya orada kalma, bilişim sisteminin parçalarının açılarak veya sökülerek fiziki olarak içine girilmesi anlamında değildir. Bilişim sisteminin sanal ortamının içine dâhil olunması, bilişim sisteminin yazılımına erişilmesi ve ulaşılmasıdır. Suç, başkasının bilgisayarındaki verilerin açılarak izinsiz olarak görüntülenmesi, bilişim sisteminde oturum açılması gibi şekillerde işlenebilir. Girme aşamasında bağlantının kablolu veya kablosuz olması, mesafe gibi kriterler dikkate alınmaz. Bir bankaya ait müşteri hesabına hukuka aykırı olarak girilerek bakılması, bir kurumun bilgisayarına ait yazılıma girilmesi, başkasına ait açık bilgisayarın içindeki verilere bakılması bu suçu oluşturmaktadır[56]. Verilerin ele geçirilmesi suçun oluşması bakımından zorunlu unsur değildir. Hukuka aykırı olarak bilişim sisteminde kalınmaya devam edilmesi yönünden bir süre şartı öngörülmemiştir. Doktrin yönünden bu konuda tartışma bulunmakla[57] birlikte, failin bilişim sistemine girdiğini fark ettiği anda sistemden çıkmamış olması suçun oluşumu için yeterli görülmektedir. Diğer taraftan, somut olaya göre bilişim

---

[54] Yargıtay 8. CD, 2015/1133 E. 2015/22729 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 25.03.2020)

[55] KOCA/ÜZÜLMEZ, **2017**, s.812.

[56] ERDOĞAN, **2010**, s.1375.

[57] ERDOĞAN, **2010**, s.1377.

sistemine girilip, girilmediği veya sistemde kalınmaya devam edilip edilmediği değerlendirmeli; suçun oluşumu soruşturma ve kovuşturma aşamasında incelenmelidir. Süre yönünden herhangi bir bağlayıcılığın olmaması, suçun fiil ve yöntem açısından tartışılmasını gerektirmektedir. Ayrıca bilişim sistemine girilen mağdur yönünden zararın oluşup oluşmamasının suçun meydana gelmesi açısından bir önemi yoktur.

B. Suçun Manevi Unsuru

Bilişim sistemine girmeyi düzenleyen TCK'nın 243'üncü maddesinin 1'inci fıkrasına göre suç sadece kasten işlenebilmektedir. Failin bir bilişim sisteminin tamamına veya bir kısmına kasıtlı olarak girmesi veya burada bilerek hukuka aykırı şekilde kalması suçu oluşturacaktır[58]. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'inci maddesi kapsamında taraf devletler "*bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman*" cezalandırmalıdır. TCK'da yer alan düzenleme Avrupa Konseyi Siber Suçlar Sözleşmesi'yle uyumludur[59]. Suçun hangi amaçla işlendiğinin ve ortaya çıkan sonucun herhangi bir önemi yoktur. Dolayısıyla, suçun meydana gelmesi açısından kast yeterli olmakla, failin eğlence, deneme veya başka bir nedene dayalı olarak suçu işlemesinin farkı bulunmamaktadır[60]. Ancak 243'üncü maddenin 3'üncü fıkrasında yer alan suçun neticesi sebebiyle ağırlaştırılmış halinde, verilerin yok olması veya değiştirilmesi halinin taksirle gerçekleşmesi gereklidir. Failin bilerek ve isteyerek verileri değiştirmesi veya bozması halinde ise TCK'nın 244'üncü maddesi değerlendirilmelidir[61]. TCK'nın 243'üncü maddesinin 4'üncü fıkrası bakımından da 1'inci fıkrada olduğu gibi kast aranmaktadır. TCK'da taksirli eylemin cezalandırılacağı ayrıca belirtilmedikçe o suçtan ceza verilemez. TCK'nın 243'üncü maddesinin 3'üncü fıkrası dışında maddede yer alan suçun gerçekleşmesinde doğrudan kast aranmaktadır[62]. Failin bilişim sistemine yönelik icra hareketlerine başlaması ancak

[58] KOCA/ÜZÜLMEZ, **2017**, s.814.

[59] ERDOĞAN, **2010**, s.1405.

[60] KARAKEHYA, **2009**, s.14.

[61] GÖNEN/ULUS/YILMAZ, **2016**, s. 230.

[62] KOCA/ÜZÜLMEZ, **2017**, s.815.

icra hareketleri tamamlanmadan sisteme girmekten vazgeçmesi durumunda gönüllü vazgeçmeden yararlanabileceği de kabul edilmektedir[63].

C. Hukuka Aykırılık Unsuru

Bilişim sistemine girme suçunun kanuni tanımında hukuka aykırılık ifadesine yer verilmiştir. Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kişi suç nedeniyle cezalandırılmaktadır. Bazı durumlarda hak sahibi, failin bilişim sisteminin bir kısmına girmesine rıza göstermiş olabilir. Bu durumda failin hak sahibinin gösterdiği rıza dışındaki alanlara girmesi hukuka aykırılık oluşturacak ve suç meydana gelecektir. Rıza, bilişim sistemi üzerinde hak sahibi olan kişi tarafından verilmelidir. Yetkisiz kişi tarafından verilen rızanın önemi bulunmamaktadır[64]. Fail eğer bir bilişim sistemine girdiği veya orada kaldığı hususunda hataya düşmüşse, bu hatasından yararlanabilir. Hukuka uygunluk sebepleri yönünden maddi koşullar bakımından kaçınılmaz bir hataya düşen fail için TCK'nın 30'uncu maddesinin 1'inci fıkrası uygulaması değerlendirilmelidir[65]. Diğer taraftan failin işlediği fiilin suç oluşturduğu hususunda hataya düşmesi de söz konusu olabileceğinden, failin TCK'nın 30'uncu maddesinin 4'üncü fıkrası uyarınca kaçınılmaz bir hataya düşüp düşmediğinin somut olaya göre incelenmesi gereklidir[66]. Kanunların verdiği yetkiye dayanarak izinsiz olarak bilişim sistemine girilmesi veya orada kalınması da hukuka uygunluk nedenidir. CMK'nın 134'üncü maddesinde yer alan "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma", 135'inci maddesinde düzenlenen "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" ve 140'ıncı maddesinde düzenlenen "Teknik Araçlarla İzleme" koruma tedbirlerinin kanunda yer alan şartlara uygun olarak gerçekleştirilmesi suç sayılmayacaktır. Sadece belirli kimselerin girmesi için oluşturulan bir internet sayfasına ya da programa, fail tarafından şifre kırılmak suretiyle erişilmesi durumunda suçun oluştuğu kabul edilir. Çünkü fail

---

63 TAŞKIN, **2008**, s.30.

64 ERDOĞAN, **2010**, s.1409.

65 APAYDIN, **2017**, s. 76.

66 ÖZÇELİK, Büşra, **Bilişim Sistemine Girme Suçu**, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2019, s.73.

tarafından bir bilişim sistemine müdahalede bulunulmakta ve şifre kırılmak suretiyle girilmemesi gerekli alana erişilmektedir[67]. Bir bilişim sistemine şifre konulmamış olması ya da bilişim sisteminin açık bırakılması, rıza verildiği anlamına gelmez. Örneğin, bir kişinin bilgisayarını eve bırakması için arkadaşına veya komşusuna vermesi durumunda şifreli olmayan bilgisayarın açılarak sistemi girilmesi durumunda rıza bulunmadığından suç oluşacaktır. Rıza ve hukuka uygunluk nedenlerinin eylem öncesinde mevcut olması zorunludur. Doktrinde tartışılan bir diğer konu ise rızanın şarta bağlı olarak verilip verilmeyeceğidir. Bilişim sistemine belirli bir amaç için girilmesi için verilen rıza sonucu sistemin farklı bir amaç doğrultusunda kullanılmasının suç oluşturmayacağı savunulmuştur[68]. Ancak bu görüşün kabul edilmesi mümkün değildir. Çünkü mağdurun faile cep telefonunu sadece sesli görüşme yapma amacıyla vermesi ancak failin mağdurun cep telefonunda yer alan programlara girmesi, telefondaki mesajlara bakması gibi fiiller bilişim sistemine girme suçunu oluşturmalıdır. Mağdurun burada gerçekleşen fiiller yönünden rızasının bulunduğunu söylemek mümkün değildir.

D. Karşılaştırmalı Hukuk

Verilen yetkinin aşımı hususunda karşılaştırmalı hukukta da düzenlemeler yer almaktadır. Amerika Birleşik Devletleri yasası olan CFAA[69]'de yetkisiz erişim dışında yetki aşımı da düzenlenmiştir. Örneğin, bir kişiden para veya başka bir değer sızdırmak amacıyla devlet bilgisayarlarına, banka bilgisayarlarına, devletlerarası veya dış ticarette kullanılan bir bilgisayara zarar verme veya gizliliğini ihlal etme tehdidinde bulunma suç olarak kabul edilmiştir[70]. Ancak yetki aşımı sonucu erişim fiilinin tamamen suç olmaktan çıkarılmadan, belirli şartlara tabi tutulması gerektiği ileri sürülmektedir. Ayrıca, CFAA eski bir kanun olması ve ihtiyaçları karşılayamaması nedeniyle eleştirilmekte, kanunda reform yapılması gerektiği tartışılmaktadır[71]. Siber suçların Amerika Birleşik

---

67 KARAKEHYA, **2009**, s. 17.

68 AKBULUT, Berrin, **Bilişim Alanında Suçlar**, 2. Basım, Adalet Yayınevi, Ankara, 2017, s. 137.

69 Computer Fraud and Abuse Act: Bilgisayar Sahtekarlığı ve Kötüye Kullanım Yasası.

70 DOYLE, Charles, "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws", **Congressional Research Service**, Yıl:2014, (s. 1-91), s. 2.

71 WHİTEHOUSE, Sheldon, "Hacking into the Computer Fraud and Abuse Act: The CFAA at 301", **The George Washington Law Review,** Yıl:2016, Cilt:84, Sayı:6, (s.1437- 1441), s. 1440.

Devletlerinde her yıl daha fazla yaygınlaşması karşısında hükümet CFAA'nın kapsamının genişletilmesi yönünde çalışmalar sürdürürken, hükümet karşıtları ise yasanın daraltılması gerektiğini ileri sürmektedir[72]. İngiltere'de verilen yetkinin açıkça tanımlanmış olması durumunda, yetki dışı amaçla sisteme girilmesi veya yetkinin dışına çıkılmasının suç oluşturacağı yargı kararlarında yer almaktadır. Rıza dışına çıkılarak bilişim sistemine girme veya orada kalma fiili suç oluşturmalıdır. TCK'da yetki aşımı konusunda güncel düzenlemelerin yapılması, yetki aşımının somut olaya göre değerlendirilmesi, her yetki aşımının suç oluşturmaması gerektiği ayrıca doktrinde tartışılmaktadır[73].

E. Suçun Özel Görünüş Biçimleri

Bilişim sistemine girme suçunun özel görünüş biçimleri teşebbüs, iştirak ve içtima başlıkları altında incelenecektir.

1. Teşebbüs

Bilişim sistemine girme suçu 6698 Sayılı Kanun ile yapılan düzenleme uyarınca seçimlik hareketli hale gelmiştir. Bu nedenle suça teşebbüs yönünden doktrinde farklı görüşler ortaya çıkmıştır. Bilişim sistemine girme suçunda teşebbüsün olmayacağını ileri süren görüşe göre suç, tehlike suçudur. Dolayısıyla bilişim sistemine hukuka aykırı olarak girme veya orada kalma fiili sonucu suç meydana gelmektedir[74]. Bir başka görüşe göre ise bilişim sistemine girme suçunda girme ve kalma fiilleri yönünden ayrı ayrı inceleme yapılmalıdır[75]. Fail bilişim sistemine hukuka aykırı olarak erişim sağlamışsa artık kalma fiili yönünden teşebbüs aranmayacaktır. Doktrindeki ağırlıklı görüş ise bilişim sistemine girme suçu bakımından teşebbüsün mümkün olduğudur[76]. Failin bilişim sistemine

---

72 WESTERHORSTMANN, Kristin, "The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Attacks, Fake Dating Profiles and Employees Who Check Facebook at Work", **University of Miami National Security & Armed Conflict Law Review**, Yıl: 2015, Cilt: 145, (s. 145-174), s. 160.

73 KARAGÜLMEZ, **2009**, s. 230.

74 YILMAZ, Sacit, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, 1. Basım, Adalet Yayınevi, Ankara, 2016, s. 190.

75 DOĞAN, Koray, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", **Hukuk ve Adalet Eleştirel Hukuk Dergisi**, Yıl: 2005, Sayı: 6-7, (s. 290-319), s. 299.

76 ERDOĞAN, **2010**, s.1413-1414.

girmeye çalışırken elinden olmayan sebeplerle sisteme girememesi durumunda teşebbüsün oluşabileceği kabul edilmelidir. Örneğin, failin mağdura e-posta veya diğer programlar aracılığıyla trojan göndermesi, mağdurun bu virüsü açmaması, silmesi nedeniyle sisteme girilememesi durumunda teşebbüs meydana gelecektir. Ancak bilişim sistemine girildikten sonra hukuka aykırı olarak kalınması durumunda teşebbüsten söz edilemez. Bilişim sistemine hukuka aykırı olarak erişim sonucunda çok kısa süre için sistemde kalınsa dahi suç tamamlanmış olacaktır[77]. Benzer durum TCK'nın 243'üncü maddesinin 3'üncü fıkrasında yer alan suçun netice sebebiyle ağırlaşmış hali için de geçerlidir. Bilişim sistemine hukuka aykırı olarak girilmesi sonucu verilerin yok olması ve değişmesi taksire dayalı olduğundan ve TCK kapsamında taksirli suçlara teşebbüs mümkün olmadığından bu fıkra yönünden tartışma bulunmamaktadır[78]. 234'üncü maddenin 4'üncü fıkrasında yer alan bilişim sistemindeki veri nakillerinin sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlenmesi bakımından da 1'inci fıkrada olduğu teşebbüsün mümkün olduğu kabul edilmelidir. Veri nakillerinin teknik araçlarla izleme mütemadi suç niteliğindedir. Fiil devam ettiği sürece suç kesintiye uğramayacaktır. Teşebbüsün mümkün olması için suçun tamamlanmamış olması gereklidir. Bu nedenle veri izleme devam ederken herhangi bir nedenle failin engellenmesi durumunda suç tamamlanmış olacaktır. Fakat fail elinde olmayan sebeplerle veri nakillerini ve transferlerini takip edememişse teşebbüs söz konusu olabilir[79]. Teşebbüsten söz edebilmek için fail tarafından fiile elverişli hareketlerle doğrudan başlanılması gereklidir. Failin fiili somut olaya göre değerlendirmeli ve sonucuna göre teşebbüs incelemesi yapılmalıdır[80]. Daha önce vurgulandığı üzere suç yönünden gönüllü vazgeçme mümkündür. Failin bilişim sistemine hukuka aykırı olarak girme amacıyla fiilde bulunması ancak sisteme girmeden kendi rızasıyla fiilden vazgeçmesi durumunda artık 234'üncü maddenin 1'inci fıkrası nedeniyle cezalandırılması söz konusu olmaz[81].

---

77 AKBULUT, **2017**, s. 150-151.

78 ÖZBEK/ DOĞAN/BACAKSIZ/TEPE, **2017**, s. 955.

79 KOCA/ÜZÜLMEZ, **2017**, s. 823.

80 KARAKEHYA, **2009**, s.19.

81 TAŞKIN, **2008**, s.30.

2. İştirak

Bilişim sistemine girme suçu birden fazla kişiyle işlenebilir. Suçun iştirak halinde işlenmesi durumunda TCK'nın 37'inci ve devamı maddeleri uygulanacaktır. Fiilin, başka birini bilişim sistemine girmeye veya orada kalmaya ikna etme şeklinde gerçekleşmesi durumunda kişi, azmettiren olarak sorumlu tutulacaktır[82]. Suça yardım eden sıfatıyla katılmak da somut olaya göre mümkündür. Bilişim sistemine erişim yetkisi olmayan şahıslara sistem şifrelerinin verilmesi, failin bu şifrelerden yararlanarak bilişim sistemine hukuka aykırı olarak erişim sağlaması durumunda şifreleri faile veren kişi yardım eden sıfatıyla suçtan sorumlu olacaktır.

İstanbul Bölge Adliye Mahkemesi tarafından verilen bir kararda *"Şüphelinin diğer şüpheli tarafından azmettirmesi ve talimatı sonucu, ... Medikal Ürün. San. ve Tic. Ltd Şti ünvanlı firmada çalıştığı sırada müştekinin kullanımına tahsis edilen bilgisayardan, hukuka aykırı olarak ve bu bilinçle, müştekinin şahsi e-posta hesabına müştekinin izni ve haberi olmaksızın erişerek ve burada kalarak bu hesaptaki şirkete ilişkin yazışmaların içeriğini ele geçirdiği ve böylece üzerlerine atılı bulunan suçu iştirak halinde işledikleri ve atılı suçun unsurları itibari ile oluştuğuna kanaat getirilerek"* bilişim sistemine girme suçundan hüküm kurulmuştur[83]. İncelenen kararda, şüphelinin müştekinin bilgisi ve rızası dışında bilişim sistemine giriş yaparak e-posta hesabında yer alan verilere ulaşması, bilişim sistemine girme suçu olarak nitelendirilmiş; yerel mahkemenin beraat kararı kaldırılarak mahkûmiyet hükmü kurulmuştur. Faili suça yönlendiren kişi suçtan azmettiren olarak sorumlu tutulmuştur.

3. İçtima

Suçların içtimaı ile ilgili düzenlemeler TCK'nın 42, 43 ve 44'üncü maddelerinde yer almaktadır. TCK'nın 43'üncü maddesi kapsamında failin aynı suç işleme kastıyla bir kişiye karşı aynı suçun temel şeklini ya da nitelikli hallerini farklı zamanlarda işlemesi durumunda zincirleme suç meydana gelir. TCK'nın 243'üncü maddesinin birinci ve üçüncü fıkraları yönünden zincirleme suç hükümleri somut olaya göre uygulama alanı

[82] KARAKEHYA, **2009**, s. 20.

[83] İstanbul BAM 26. CD, 2019/141 E. 2019/368 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 25.03.2020)

bulabilir. Failin bir bilişim sistemine farklı zamanlarda hukuka aykırı olarak girmesi durumunda zincirleme suç oluşur ve failin cezası dörtte birinden dörtte üçüne kadar arttırılır[84]. Failin sistemde kalma süresi zincirleme suç hükümlerinin uygulanması yönünden önem arz etmektedir. Süre, failin aynı suç işleme kastıyla hareket edip etmediğini belirlemektedir. Doktrindeki bir görüşe göre, failin aynı suç işleme kastıyla hareket etmeyeceği kadar uzun süre sistemde kalması durumunda gerçek içtima hükümleri uygulanmalıdır[85]. Bu durumda fail yönünden, bilişim sistemine hukuka aykırı her erişim için ayrı cezaya hükmedilmelidir. Bir diğer görüşe göre ise fail çok kısa zaman aralığında sisteme girip çıkıyorsa, zincirleme suç dolayısıyla tek bir cezaya hükmedilerek ceza arttırılmalıdır[86]. Zincirleme suç yönünden yapılacak tespitlerde, suçta kullanılan teknik sistemin özelliğine göre de inceleme yapılmalıdır. Bilişim sisteminde kalma fiili mütemadi suçtur. Fiilin tipikliği nedeniyle kalma süresi kesilmediği müddetçe failin kastının tek suça yönelik olduğu kabul edilecektir. Diğer taraftan failin farklı şahıslara ait bilişim sistemine hukuka aykırı olarak girmesi durumunda mağdur sayısı kadar suç oluşacaktır[87]. Bilişim sistemine girme suçu başka bir suçun unsuru ve nitelikli hali olabilir. Bu durumda bileşik suç hükümleri uygulanır. Örnek olarak bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen nitelikli hırsızlık ve nitelikli dolandırıcılık suçları gösterilebilir[88]. Bu suçlar dışında da bilişim sistemlerini kullanma yoluyla işlenen suçlar bulunmaktadır. Bilişim sistemine hukuka aykırı olarak erişim sonucu mağdurun özel hayatının gizliliği ihlal edilir veya haberleşmesi engellenirse fikri içtima hükümleri uygulanacaktır. Aynı durum haberleşmenin gizliliği için de geçerlidir[89]. TCK 243 ve 244 arasındaki ilişkinin de açıklanması zorunluluğu bulunmaktadır. Doktrinde bir takım

---

84 AKBULUT, **2017**, s. 152.

85 ERDOĞAN, **2010**, s.1417.

86 SOYASLAN, Doğan, **Ceza Hukuku Özel Hükümler,** 11. Basım, Adalet Yayınevi, Ankara, 2016, s. 638.

87 ERDOĞAN, **2010**, s.1417.

88 TCK madde 142/2: Hırsızlık suçunun, bilişim sistemlerinin kullanılması suretiyle işlenmesi,

TCK madde 158/1.f: Dolandırıcılık suçunun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi halinde.

89 EKİCİ ŞAHİN, Meral/KORUCULU, Irmak, "Bilişim Sistemine Girme Suçu, Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme", **DEÜ Hukuk Fakültesi Dergisi**, Yıl: 2019, Cilt: 21, Özel Sayı, (s. 585-626), s. 620-621.

görüşe göre iki suç arasında fikri içtima hükümleri uygulanmalıdır[90]. Diğer bir görüşe göre ise failin kastına göre hareket edilmeli, 244'üncü maddede yer alan suç olmuşmuşsa artık 243'üncü maddeye göre ceza verilmemelidir[91]. TCK 243 ve 244 arasındaki bağı tüketen ve tükenen norm ilişkisi olarak kabul edenler olduğu gibi bu bağın bulunmadığını, eylemler arasındaki zamansal farka göre hareket edilmesi gerektiğini ileri sürenler bulunmaktadır[92].

Ankara Bölge Adliye Mahkemesi'nin bir kararında *"Dosyanın bir bütün halinde incelenmesinde, sanığın birden fazla kez aynı kast altında katılanın yetkilisi olduğu ve ...Bilişim Sistemleri Ltd. Şti' nin internet sitesine girerek kendi savunmasına göre orada tespit ettiği güvenlik açıklarını firma yetkililerine göstermek amacıyla veri yerleştiği ve verileri bozduğu iddia edilmiş ise de, sanığın katılana ait bilişim sistemine izinsiz girdiği ancak veri yerleştirdiğine ve verileri bozduğuna dair delil bulunmadığından, sanığın eyleminin TCK'nın 244/2 maddesinde belirtilen bilişim sistemine izinsiz girerek veri yerleştirme ve bozma suçunu değil, sadece bilişim sistemine hukuka aykırı olarak girme suçunu oluşturduğu ve sanığın aynı suç işleme kararını icrası kapsamında değişik zamanlarda aynı mağdura karşı aynı suçu birden fazla kez işlediği, bu nedenle de hakkında zincirleme suç hükümlerinin uygulanması gerektiği"* belirtilmekle, suçun bilişim sistemine hukuka aykırı girilmesi olduğu, sisteme herhangi bir veri yerleştirilmediği ya da var olan verilerin bozulmadığı, bu nedenle TCK'nın 244'üncü maddesinin 2'inci fıkrasında yazılı olan suçun somut olayda meydana gelmediği, failin bilişim sistemine girme suçundan zincirleme suç hükümlerine göre cezalandırılması gerektiği kabul edilmiştir[93]. Yargıtay'ın bir ilamında "*Sanık hakkında düzenlenen iddianamede; sanığın, mağdura ait facebook ve telefon hesaplarına rızası dışında girerek bilişim sistemine girme, mağdurun orijinal fotoğrafları ile birlikte çıplaklık içeren fotoğrafları mağdura aitmiş gibi internette paylaşarak görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçlarını işlediği iddia edilmiş olup, sanığa*

90 KOCA/ÜZÜLMEZ, **2017**, s. 819.

91 YENİDÜNYA, **2005**, s. 1039.

92 DÜLGER, Murat Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku**, 4. Basım, Seçkin Yayınevi, Ankara, 2014, s. 384.

93 Ankara BAM 8.CD, 2017/207 E. 2018/439 K. (Uyap Bilişim Sistemi-Erişim Tarihi: 20.03.2020)

yüklenen farklı eylemlerden dolayı ayrı ayrı hüküm kurulması gerektiği, TCK'nın 44/1. madde ve fıkrasındaki fikri içtima koşullarının bulunmadığı gözetilmeden, "bilişim sistemlerine girme ve özel hayatın gizliliğini ihlal suçlarının sabit olmakla birlikte tek bir eylem ile icra edildiğinden TCK'nın 44. maddesinin bu suçlar yönünden tatbik edilmesine" biçimindeki yasal ve yeterli olmayan gerekçelerle yazılı şekilde görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçundan mahkûmiyet hükmü kurulması" bozma nedeni yapılmıştır[94]. Failin fiili sonucu bilişim sistemine girme suçu dışında oluşan diğer suçlar bakımından inceleme yapılmalı, sonucuna göre TCK 44 değerlendirilmelidir. Aksi takdirde fikri içtima hükümlerine uygun olmayan, eksik mahkûmiyet hükmü kurulması söz konusu olacaktır.

III. MUHAKEME USULÜ VE YAPTIRIM

Bilişim sistemine girme suçunun temel şekli ile nitelikli ve neticesi sebebiyle ağırlaşmış halinin yargılaması açısından görevli mahkeme 5235 sayılı Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11'inci ve 12'inci maddeleri uyarınca Asliye Ceza Mahkemeleridir. Yetkili mahkeme, suçun işlendiği yer mahkemesidir. Suçun seçimlik hareketli ve temadi eden niteliği gereği, temadinin kesildiği yer mahkemesi yetkili olacaktır. Teşebbüs halinde, son icra hareketinin yapıldığı yer, zincirleme suç durumunda ise son suça ilişkin fiilin işlendiği yer mahkemesi yetkilidir. Bilişim suçları sanal ortamda işlendiğinden, saldırılar çoğunlukla uluslararası nitelik göstermektedir. Bu nedenle yetkili mahkemenin tespitinde zaman zaman sorunlar yaşanmaktadır[95]. Bilişim sistemine girme suçunun temel şekli, nitelikli ve neticesi sebebiyle ağırlaşmış hali resen takip edilen suçlardır. Ancak suça ilişkin yaptırımların ağırlığının fazla olmaması nedeniyle şikâyete tabi olması gerektiği doktrinde tartışılmaktadır[96]. Suçun koruduğu hukuki menfaat dikkate alındığında suçun resen soruşturulması yerindedir. TCK'nın 66'ıncı maddesi gereği "*beş yıldan fazla olmamak üzere hapis veya adlî para cezasını gerektiren suçlarda*" dava

[94] Yargıtay 12. CD, 2018/8261 E. 2019/6852 K. (Uyap Bilişim Sistemi, Erişim Tarihi 21.08.2020)

[95] GÖKCEN, Ahmet/ BALCI, Murat/ ALŞAHİN, Mehmet Emin/ÇAKIR, Kerim, **Ceza Muhakemesi Hukuku**, 3. Basım, Adalet Yayınevi, Ankara, 2018, s. 180.

[96] KOCA/ÜZÜLMEZ, **2017**, s.819.

zamanaşımı süresinin 8 yıl olduğu kabul edilmiştir. Dolayısıyla bilişim sistemine girme suçu bakımından dava zamanaşımı süresi fiilin işlendiği tarihten itibaren sekiz yıldır.

TCK'nın 243'üncü maddesinin 1'inci fıkrasında yer alan suçu işleyen fail bir yıla kadar hapis veya adli para cezasıyla cezalandırılacaktır. Madde metninde 'veya' ifadesi yer aldığından, hâkim seçimlik cezalardan yalnız birine hükmedecektir. 2'inci fıkrada fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek cezanın yarı oranına kadar indirileceği belirlenmiştir. Burada indirim yapma konusunda hâkimin takdir yetkisi bulunmamaktadır. 3'üncü fıkrada yer alan suçun netice sebebiyle ağırlaşmış halinde suçun cezası altı aydan iki yıla kadar hapis cezasıdır. Bu fıkra kapsamında, sisteme girdikten sonra sistemin içerdiği verilerin yok olması veya değişmesi gereklidir. Ayrıca suçun temel şekline nazaran 3'üncü fıkrada seçimlik ceza olarak adli para cezası öngörülmemiştir. 4'üncü fıkrada bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleme suçunun cezası bir yıldan üç yıla kadar hapis cezasıdır. İlk üç maddenin ihlal edilmesi durumunda ise fail 3'üncü maddeye göre cezalandırılacaktır[97].

SONUÇ

Bilişim teknolojileri alanında yaşanan gelişmeler insan yaşamında köklü değişiklikler yaratmıştır. Bu alanda yaşanan gelişmeler yeni suç tiplerinin de meydana gelmesine, bilişim suçlarının hukuk mevzuatlarına girmesine neden olmuştur. Ancak suçların değişkenliği ve gelişimi karşısında yasal mevzuatın yeterli olduğunu söylemek mümkün değildir. Bilişim suçlarının failleri, çoğu zaman dijital ortamda fiziki ortama göre daha kolay faaliyet göstermektedir. Suçlarla mücadele edilmesi amacıyla daha yoğun çalışma yapılması, gerektiğinde uluslararası işbirliğine gidilmesi zorunluluğu ortaya çıkmaktadır. Çünkü bilişim suçları giderek uluslararası boyut kazanmaktadır. Türkiye'de işlenen bilişim suçlarında failler genellikle yurt dışında bulunan servis sağlayıcılardan ve sunuculardan yararlanmaktadır. Bu nedenle adli yardımlaşma

[97] KAYAER, Nebahat, "Türk Hukukunda Bilişim Sistemine Girme Suçu", **Ceza Hukuku Dergisi**, Yıl: 2019, Sayı: 39, (s.83-128), s. 122.

boyutunun geliştirilmesi zorunludur. Aksi takdirde soruşturmaların uzun yıllar sürmesi ve sonuç alınamaması söz konusu olacaktır.

Bilişim sistemine girme suçu TCK'da ayrı suç olarak düzenlenmiştir. Suç, özel hayatın gizliliğinin ve kişisel verilerin korunması, haberleşme özgürlüğüne haksız müdahalelerin engellenmesi gibi birçok amaca hizmet etmektedir. 2016 yılında 6698 sayılı kanun ile yapılan değişiklik sonucu sadece bilişim sistemine girmenin veya orada kalmanın suç sayılması ile birlikte düzenlemenin kapsamının genişlemesi olumludur. Ancak 6698 sayılı kanun ile TCK 243'e eklenen veri nakillerinin hukuka aykırı şekilde izlenmesini içeren 4'üncü fıkra ile madde karma düzenleme halini almıştır. TCK 243 başlığı ile içerik bir bakıma uyumsuz hale gelmiştir. Doktrinde de bu düzenlemenin eklenmesi sıklıkla eleştirilmektedir. Avrupa Konseyi Siber Suç Sözleşmesi'ne uyum sağlamak için eklenen veri nakillerinin hukuka aykırı şekilde izlenmesi suçunun ayrı bir fıkra olarak düzenlenmesinin yerinde olacağı kanaatindeyiz. Diğer fıkralarda yer alan suçun temel şekli, daha az cezayı gerektiren hal ve neticesi sebebiyle ağırlaşmış hale ilişkin düzenlemenin uyumlu olduğu söylenebilir.

TCK'nın 243'üncü maddesinin 1'inci fırkasında yer alan bilişim sistemine girme suçunun temel şeklinin yeterli caydırıcılığının bulunduğu söylemek mümkün değildir. Suç için öngörülen adli para cezası veya hapis cezası, suçun tipikliği ve korunan hukuki menfaat dikkate alındığında yetersiz kalmaktadır. Suç, özel hayatın ve haberleşmenin gizliliği, malvarlığı haklarının korunması gibi temel hukuki değerleri muhafaza eden temel suç tipini oluşturmaktadır. Suçla kısmen bilişim sistemlerinin güvenliği de koruma altına alınmaktadır. Suçun belirli bir bedel karşılığı kullanılan bilişim sistemleri üzerinde işlenmesi durumunda, 243'üncü maddenin 2'inci fıkrasında ceza indirimi öngörülmüştür. Ancak bu fıkra tartışmaya açıktır. Bedeli ödenmeksizin bir bilişim sisteminde kalma fiilinin cezayı hafifleten değil ağırlaştıran bir nitelikli hal olarak düzenlenmesi kanaatindeyiz. Çünkü fail, mağdurun belirli bir bedel ödediği sisteme hukuka aykırı olarak girmekte; mağdurun malvarlığına yönelik bir saldırı da gerçekleştirmektedir. Diğer taraftan suçun meydana gelmesi yönünden herhangi bir verinin ele geçirilmesi, zararın oluşması gibi unsurlara yer verilmemiştir. Düzenlemenin bu bakımdan caydırıcılığının olduğunu söylemek mümkündür. 243'üncü maddenin 3'üncü fıkrasında verilerin yok

olması veya değişmesi neticesi sebebiyle ağırlaşmış hal olarak düzenlenmiş, bilişim sistemi dışarıdan gelebilecek müdahalelere karşı korunmuştur. Bu kapsamda bilişim sistemine taksirle girme suçunun da ayrıca yasal mevzuatta düzenlenmesi yerinde olacaktır. 243'üncü maddenin 4'üncü fıkrasında öngörülen cezanın alt ve üst sınırının temel şekle nazaran daha ağır öngörüldüğü anlaşılmaktadır. Veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleme suçunun alt ve üst ceza sınırının diğer fıkralara nazaran daha ağır düzenlenmiş olması; bilişim sistemlerinin hukuka aykırı olarak izlenmesinin önüne geçilmesi açısından olumludur.

Bilişim suçlarıyla mücadele açısından gerekli eğitimi almış adli bilişim personelinin ve konusunda uzmanlaşmış Cumhuriyet savcılarının, ihtisas mahkemelerinin bulunması zorunlu görülmektedir. Delillere ve verileri ulaşma hızı, suç bakımından yapılacak tespitler açısından önemlidir. Bölge Adliye Mahkemeleri ve Yargıtay kararlarında da bu durum ortaya çıkmaktadır. Bu nedenle kolluk personeli ve yargı teşkilatı bilişim suçları yönünden sürekli eğitilmeli, hukuki ve teknik bilgiler değişen teknolojiye uyum sağlamak amacıyla güncellenmelidir.

KAYNAKÇA

AKBULUT, Berrin, **Bilişim Alanında Suçlar**, 2. Basım, Adalet Yayınevi, Ankara, 2017.

APAYDIN, Cengiz, **Bilişim Suçları ve Bilişim Ceza Hukuku**, 1. Basım, Acar Matbaacılık, İstanbul, 2017.

APİŞ, Özge, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri", **Yasama Dergisi**, Yıl: 2018, Sayı: 37, (s. 49-86).

ATASOY, Fahri, "Kültürler Üzerinde Bilişim Devriminin Etkileri", **Modern Türklük Araştırmaları Dergisi**, Yıl:2007, Cilt: 4, Sayı: 2, (s.163-178).

AVŞAR, B. Zakir/ÖNGÖREN, Gürsel, Bilişim Hukuku, **Türkiye Bankalar Birliği,** Yıl:2010, Yayın No: 270, s.134.

BOSS, Richard W, "Intranet and Extranet", **PLA Tech Notes, American Library Association**, Yıl: 2010, (s.1-4).

DOYLE, Charles, "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws", **Congressional Research Service**, Yıl:2014, (s. 1-91).

DÜLGER, Murat Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku**, 4. Basım, Seçkin Yayınevi, Ankara, 2014.

EKER, Ö. Umut, "Türk Ceza Hukuku'nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 s. Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", **Türkiye Barolar Birliği**, Yıl:2006, Sayı:62, (s. 123-131).

EKİCİ ŞAHİN, Meral/KORUCULU, Irmak, "Bilişim Sistemine Girme Suçu, Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme", **DEÜ Hukuk Fakültesi Dergisi**, Yıl: 2019, Cilt: 21, Özel Sayı, (s. 585-626).

ERDAĞ, Ali İhsan, "Bilişim Alanında Suçlar (Türk ve Alman Hukukunda)", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Yıl:2010, Cilt:14, Sayı: 2, (s.275-303).

ERDOĞAN, Yavuz, "Bilişim Sistemine Girme ve Kalma Suçu", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,** Yıl:2010, Cilt: 12, Özel Sayı, (s.1363-1433).

GÖKCEN, Ahmet/ BALCI, Murat/ ALŞAHİN, Mehmet Emin/ÇAKIR, Kerim, **Ceza Muhakemesi Hukuku**, 3. Basım, Adalet Yayınevi, Ankara, 2018.

GÖNEN, Serkan/ULUS, Halil İbrahim/ YILMAZ, Ercan Nurcan, Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, **Bilişim Teknolojileri Dergisi**, Yıl: 2016, Cilt:9, Sayı:3, (s. 229-236).

KARAGÜLMEZ, Ali, **Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri**, Seçkin Yayınevi, Ankara, 2009.

KARAKEHYA, Hakan, Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", **TBB Dergisi**, Yıl: 2009, Sayı:81, (s.1-24).

KAYAER, Nebahat, "Türk Hukukunda Bilişim Sistemine Girme Suçu", **Ceza Hukuku Dergisi**, Yıl: 2019, Sayı: 39, (s.83-128).

KETİZMEN, Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2008.

KOCA, Mahmut/ÜZÜLMEZ, İlhan, **Türk Ceza Hukuku Özel Hükümler**, 4. Basım, Adalet Yayınevi, Ankara, 2017.

KOÇAK, Hüseyin/DANDİN, Ali Nazmi, "Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri", **Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi**, Yıl:2017, Cilt: 19, Sayı: 1, (s. 137-152).

KURT, Levent, **Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanununda Uygulaması**, Seçkin Yayınevi, Ankara, 2005.

MAHMUTOĞLU, Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Yıl:2013, Cilt: 71, Sayı: 1, (s. 855-889).

MALKOÇ, İsmail, **Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu**, Ankara, Malkoç Kitabevi, 2. Cilt, 2007.

ÖZBEK, Veli Özer/ DOĞAN, Koray/BACAKSIZ, Pınar/TEPE, İlker, **Türk Ceza Hukuku Özel Hükümler**, 11. Basım, Seçkin Yayınevi, Ankara, 2017.

ÖZÇELİK, Büşra, **Bilişim Sistemine Girme Suçu**, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2019.

TAŞKIN, Şaban Cankat, **Bilişim Suçları**, 1. Basım, Beta Yayınları, İstanbul, 2008.

TAŞKIN, Şaban Cankat, "Bilişim Hukuku Uluslararası Uyuşmazlıklar", **Türkiye Barolar Birliği Dergisi**, Yıl: 2009, Sayı:85, (s. 332-372).

TEKELİ, Ömer, "Bilişim Suçlarıyla Mücadelede Polisin Yeri", **Sayder Dış Denetim Dergisi**, Sayı:2011 Temmuz-Ağustos-Eylül, (s.183-192).

TEZCAN, Durmuş / ERDEM, Mustafa Ruhan / ÖNOK, R. Murat, **Teorik ve Pratik Ceza Özel Hukuku**, Seçkin Yayınevi, Ankara, 2018.

TRIPATHI, Esha/ TRIPATHI, Abhay/YADAY, Mithilesh Kumar Singh, "Role of Information Technology in Cyber Crime and Ethical Issues in Cyber Ethics", **International Journal of Business and Research (IJBER)**, Yıl: 2016, Cilt: 10, (s. 1-5).

WESTERHORSTMANN, Kristin, "The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Attacks, Fake Dating Profiles, and Employees Who Check Facebook at Work", **University of Miami National Security & Armed Conflict Law Review**, Yıl: 2015, Cilt: 145, (s. 145-174).

WHİTEHOUSE, Sheldon, "Hacking into the Computer Fraud and Abuse Act: The CFAA at 301", **The George Washington Law Reviewer,** Yıl:2016**,** Cilt:84, Sayı:6, (s.1437- 1441).

YAZICIOĞLU, Yılmaz, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi ", **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Yıl: 2005, Cilt :2, Sayı : 2, (s. 401-409).

YAZICIOĞLU, Yılmaz, "Hackerler ve Bilişim Sistemine Girme Suçu", Ord.Prof. Dr. Sulhi Dönmezer Armağanı, Yıl: 2008, Cilt:1, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, **Atatürk Araştırma Merkezi ve Türk Ceza Hukuku Derneği Yayını**, (s. 1239-1261).

YENİDÜNYA, A. Caner/DEĞİRMENCİ, Olgun, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, 1. Basım, Legal Yayıncılık, İstanbul, 2003.

YENİDÜNYA, A. Caner, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu"**, Legal Fikri ve Sınai Haklar Dergisi**, Yıl:2005, Sayı:4, (s.1018-1042).

YILMAZ, Zahit/ APİŞ, Özge, "Karşılıksız Yararlanma Suçu (TCK m.163)", **MÜHFHAD**, Yıl: 2013, Cilt: 19, Sayı: 2, (s.1749-1779.)

YILMAZ, Sacit, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, 1. Basım, Adalet Yayınevi, Ankara, 2016.