[H]BİLİŞİM SİSTEMİNE GİRME VE KALMA SUÇU

Dr. Yavuz ERDOĞAN[*]

1. GENEL OLARAK

Bilişim[1] sistemlerine özgü yasadışı eylemlerin içinde en yaygın olanı

H Hakem incelemesinden geçmiştir.

* Erzurum 9'uncu Kolordu Komutanlığı Askeri Savcısı

1 Bilişim Kavramı; Türkiye'de ilk kez bilgisayar bilimleri profesörü Prof. Dr. Aydın Köksal tarafından kullanılmıştır. Prof.Dr. Aydın Köksal "bilişim" terimini "bilmek" eyleminden ad olarak türettiğini belirtmiştir (Aydın **Köksal**, Adı Bilgisayar Olsun, Cumhuriyet Kitapları, Bilişim Yazıları, Ankara, 2010, s. 44).

Bilişim kavramına mevzuatımızda ilk kez 1989 Türk Ceza Kanunu Ön Tasarısında (TCKÖT) rastlanmaktadır. Ancak ne var ki 765 S. TCK'da, bilişim alanında suçları düzenleyen, 525a ile 525d arasındaki maddelerde bilişim kavramı yer almamaktadır. Madde metinlerinde yer almayan bu kavrama, bilişim suçlarıyla ilgili maddelerin yer aldığı bap olan 11'inci babın başlığında "Bilişim Alanında Suçlar" başlığıyla yer verilmiştir.

Bilişim kavramı Artuk/Gökçen/Yenidünya*;* "*insanların teknik, ekonomik, sosyal, kültürel, hukuksal veya 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*" şeklinde tanımlarken, Yazıcıoğlu; *"bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır"* şeklinde tanımlamıştır. Bilişim terimleri sözlüğünde ise; *"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimidir"* şeklinde tanımlanmıştır (Mehmet Emin **Artuk/**Ahmet **Gökçen/**Ahmet Caner **Yenidünya,** Türk Ceza Kanunu Şerhi, 5. C., Turhan Kitapevi, Ankara, 2009, s. 4643; Recep Yılmaz **Yazıcıoğlu**, Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile, İstanbul , Alfa Yayınevi, 1997, s. 131; Aydın **Köksal,** Bilişim Terimleri Sözlüğü, Türk Dil Kurumu Yayınları, Ankara Üniversitesi Basımevi, Ankara, 1991, s. 28).

yetkisiz erişimdir[2]. Günümüzde kişilerin özel mülklerine girmek nasıl hakim/savcı izni olmadan mümkün olmamakta ise, yine kişilerin bilişim sistemlerine yetkisizce ulaşılması da kişinin özel mülküne ya da şahsiyetine taciz olarak kabul edilmektedir. Bilişim sistemlerine yönelik bu tür müdahalelerin artması, sistemlerin yetkisiz müdahalelerden korunmasını, cezalandırılabilir bir fiil olarak nitelendirilmesini gündeme getirmiştir[3].

Ekonomik yaşamda bu suç, daha çok şirketlerin iç yazışmalarına ve ticari sırlarına ulaşmak için kullanılmaktadır[4]. Ancak burada unutulmamalıdır ki, özellikle internette olduğu üzere herkesin kullanımına açık sistemlere girmek, buralardan bilgi edinmek suç olarak kabul edilemez[5].

Biz, suçta ve cezada kanunilik ilkesini de dikkate alarak, bilişim bilim dalı uzmanı olmadığımızdan bilişim kavramını tanımlamıyor, bilişimin temel unsurlarının verilerin işlenebilmesi, saklanabilmesi ve aktarılabilmesi olduğunu belirtmekle yetiniyoruz. Diğer bir değişle, veri işlemenin, veri saklamanın ve veri iletişiminin yapılabilmesi halinde bilişimin olduğu düşüncesindeyiz. Kanaatimizce, bilişim kavramının değerlendirilmesinde sorun yaşayan yargı mercilerinin yapması gereken şey, bilişim bilim dalı uzmanlarından bilirkişi olarak faydalanmak suretiyle sorunu çözmek olmalıdır.

Bilişimin temel özelliklerinden yola çıkarak bilişim sistemini de veri iletişimi yapabilen, verileri saklayabilen ve veri depolayabilen sistemler olarak kabul etmek gerekmektedir. Nitekim, bilişim sistemini Türk ceza hukukunda ilk kez tanımlayan, Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkındaki Yönetmelik 20.092011 tarihinde Resmi Gazete'de yayınlanmış olup, bu yönetmeliğin tanımları belirleyen 3(1)-b maddesinde *"Bilişim sistemi: Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi"* ifade eder şeklinde tanımlama yapılmıştır.

2 Rizgar Mohammed **Kadir**, "The Scope and the Nature of Computer Crimes Statutes A Critical Comparative Study", German Law Journal, June, 2010. s. 626.

3 Muammer **Ketizmen**, Türk Ceza Hukukunda Bilişim Suçları, Ankara Adalet Yayınevi, 2008, s. 79.

4 Gürsel **Öngören**, İnternet Hukuku, İstanbul, Öngören Hukuk Yayınları, Yayın No:1, 2006, s. 46.

5 Benzer açıklamalar için bknz. Stein **Schjolberg**/Amanda M. **Hubbard,** "Harmonizing National Legal Approaches on Cybercrime", International Telecommunication Union WSIS Thematic Meeting on Cybercrime Geneva 28 June- 1 July 2005, s. 11.

Bilişim sistemine girme suçu ile bir nevi "engelleme suçu" yaratılmak istenmektedir. Zira bilişim suçlarının büyük bir çoğunluğu sisteme girilmek suretiyle başlamaktadır[6].

Bilişim sistemine girme suçu, failin hedef dosya ya da programlara izinsiz giriş yapması halinde ortaya çıkmaktadır[7]. Diğer bir değişle "girmek" kavramından, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesi anlaşılmaktadır[8]. "İzinsiz erişim" Avrupa Komisyonu tarafından da, bilgisayar sistemlerinin bir bölümüne ya da tümüne yapılan izinsiz erişimleri tanımlamak için kullanılmıştır[9]. Sisteme erişim yöntemi önemli değildir[10]. BM kitapçığına göre, giriş ya da erişim genellikle ağ bağlantıları boyunca uzak bir bölgeden pek çok farklı yollarla yapılmaktadır. Fail erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanabileceği gibi, var olan güvenlik önlemlerinde ki boşlukları da kullanabilir[11]. Ağ üzerinden sisteme girmek için birçok yöntem kullanabilir; bir virüs kullanarak veya sistemin açık kapıları zorlanarak giriş yapılabilir[12].

Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da

---

6 Recep Yılmaz **Yazıcıoğlu**, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını, Ankara 2009, s. 81.
Benzer açıklamalar için bknz. Kubilay **Taşdemir**, Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara, Cantekin Matbaacılık, 2009, s. 153; **Öngören**, 46.

7 **Kadir**, s. 626.

8 Cüneyd **Er**, "Bilişim Suçları", Bilişim Teknolojisi Hukuku Gündemi, 2003-2004, İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi Yayını, 2004, s. 24.

9 Anne **Flanagan**, "The Law and Computer Crime: Reading the Script of Reform", İnternational Journal of Law and Information Technology, Vol:13, No:1, Oxford University Press, 2005, s. 110.

10 Füsun **Sokullu Akıncı**, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi" İnternet Özel Bölümü, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı:1-2, İstanbul, 2001, s. 15.

11 **Kadir,** s. 626.

12 Elif **Avar,** "Bilgisayar Suçları ve Virüsler", http://arsiv.aksiyon.com.tr/arsiv/233/pages/dosyalar/dos1.html

tanımlanır[13]. Hukuk doktrinde "girme" yerine "erişim" kavramının kullanılmasının uygun olacağı zira eylemin sanal bir ortama yönelik olduğu belirtilmektedir[14]. Biz de bu düşünceye katılmaktayız. Ancak kanunda "girme" kavramının kullanılması nedeniyle çalışmamızda, kendi görüşlerimizi ifade ederken "girme" kavramını; başka kaynaklara yaptığımız atıflarda ise, kaynağın orijinalliğini bozmamak ve yazarın düşüncesine saygı göstermek adına, kaynakta kullanılan kavramı kullandık. Bu noktada belirtmeliyiz ki, TCK'da girme kavramı kullanılmasına rağmen 5651 s. Kanun'a dayanılarak çıkarılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul 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[15] bağlanarak kullanım olanağı kazanılmasını ifade eder"* şeklinde tanımlanmıştır.

Bilişim sistemine girmek (ve orada kalmaya devam etmek) suçu, Türk ceza hukukunda ilk kez 5237 s.TCK ile düzenlenmiştir. Daha önce 1997, 2000 ve 2003 TCKÖT'larında düzenlenen bu suç en nihayetinde 5237 s. Kanun ile ceza normu halini almıştır. Böylece hukukumuzdaki önemli bir boşluk da doldurulmuş, doktrindeki eleştiriler[16] karşılanmıştır[17].

---

13 **Schjolberg/Hubbard**, s. 11.

14 Özbek **Veli Özer/Kanbur** Nihat/**Doğan** Koray/**Bacaksız** Pınar/**Tepe** İlker, Türk Ceza Hukuku Özel Hükümler, Ankara, Seçkin Yayıncılık, 2010, s. 900; **Karagülmez** Ali, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, Ankara, Seçkin Yayınevi, 2009, s. 169; **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4626, 4631.

15 5651 s. Kanun'a dayanarak çıkarılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in tanımları açıklayan 3 (1) i) maddesinde ve 01.11.2007 tarihinde yayınlanan İnternet Toplu Kullanım Sağlayıcılar Hakkındaki Yönetmelik'in tanımları belirleyen 3 (1) f) maddesinde internet ortamı *"Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı ifade eder"* şeklinde tanımlanmıştır.

16 Örneğin; Ünver *"Bir kimsenin kasten ve haksız biçimde bir bilgisayar sisteminin tamamına veya bir kısmına erişmesini cezalandıran bir suç tipi düzenlenmelidir"* demiştir (Yener **Ünver**, "Türk Ceza Kanunu'nun ve Ceza Kanunu (2000) Tasarısının İnternet Açısından Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası İnternet özel Bölümü, Cilt:LIX, Sayı:1-2, 2001, s. 91).

TCK'nın 243 (1) maddesinde, bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme ve orada kalmaya devam etme fiili cezalandırılmıştır. Maddenin ikinci fıkrasında bu fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi durumu cezayı indirmeyi gerektiren hal olarak kabul edilmiş ve cezanın yarı oranına kadar indirilebileceği belirtilmiştir. Maddenin son fıkrasında ise bu fiil nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi durumu cezayı artırmayı gerektiren hal olarak kabul edilmiştir. Kanaatimizce özellikle bilişim korsanlarına (hacker) karşı etkili olabilecek bu düzenleme son derece yerinde bir düzenlemedir[18].

TCK'nın 243'üncü maddesinin TBMM Genel Kurulu'ndaki görüşmelerinde önemli değişiklikler yapılmıştır. Verilen önergeyle 5237 s. TCK'nın İkinci Kitabının, Üçüncü Kısmının Onuncu Bölüm başlığı, "Bilişim Alanında Suçlar" olarak değiştirildiği gibi, 243'üncü maddenin (1) numaralı fıkrasındaki, "giren veya kalmaya devam eden" ibaresi, "giren ve kalmaya devam eden" şeklinde ve fıkradaki "iki yıla kadar hapis veya adli para cezası" da, "bir yıla kadar hapis veya adli para cezası" olarak değiştirilmiş, 243'üncü maddenin (3) numaralı fıkrasındaki "iki yıldan dört yıla kadar

---

17 Benzer açıklamalar için bknz. Levent **Kurt**, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları, Ankara, Seçkin Yayınevi, 2005, s. 146; Osman **Yaşar**/Hasan Tahsin **Gökçan**/ Mustafa **Artuç,** Yorumlu, Uygulamalı Türk Ceza Kanunu, Cilt:5, Ankara, Adalet Yayınevi, 2010, s. 6737; Hayati **Pallı,** Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Kayseri, 2008, s. 152; Recep Yılmaz **Yazıcıoğlu**, "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi" Hukuk ve Adalet Eleştirel Hukuk Dergisi, Yıl:1, Sayı:1, Ocak-Mart 2004, s. 177.

18 Benzer açıklamalar için bknz. Murat Volkan **Dülger**, "Yeni Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları ve Bu Suçlarla Mücadelede Alınması Gereken Önlemler" 14-15 Mayıs 2005 Polis Bilişim Sempozyumu, Emniyet Genel Müdürlüğü Yayını, Kataloğ No:395, s. 201; Recep Yılmaz **Yazıcıoğlu**, "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi" Hukuk ve Adalet Eleştirel Hukuk Dergisi, Yıl:1, Sayı:1, Ocak-Mart 2004, s. 176, 177; Benzer açıklamalar için bknz. Olgun **Değirmenci**, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", Türkiye Barolar Birliği Dergisi, Yıl:18, Sayı:58, Mayıs-Haziran 2005, s. 204.

hapis cezasına" ibaresi ise, "altı aydan iki yıla kadar hapis cezasına" şeklinde değiştirilmiştir[19].

Maddenin başlığı "bilişim sistemine girme" konulmuş, bilişim sistemine girmenin önemli olduğu düzenleme ile anlatılmaya çalışılmıştır. Bu anlamda bu maddede düzenlenen suç şekli bir suçtur. Madde lafzına göre sisteme girmenin ve sistemin içinde kalmaya devam etmenin hukuka aykırı olarak gerçekleşmesi halinde suç oluşacaktır. Ancak maddenin "Bilişim Sistemine Girme" şeklindeki kenar başlığı sanki madde ile başlı başına bilişim sistemine girme fiilinin cezalandırıldığı izlenimi vermesi nedeniyle yanıltıcıdır[20]. Bu nedenle biz makalemizde bu suçu isimlendirirken (konu başlığını belirlerken) madde içeriğini tam olarak karşılayabilmesi için "bilişim sistemine girme ve kalma" şeklinde isimlendirmeyi uygun bulduk[21].

TCK'nın 243'üncü maddesiyle AKSSS'nin 2'nci maddesinde[22] öngörülen hukuka aykırı erişimin önüne geçilmesi amaçlanmaktadır[23].

---

19 Değişiklik önergesinin gerekçesinde; *"Suç tanımlarında belirliliği sağlamak ve ceza miktarlarını işlenen fiilin ağırlığına uygun olarak belirlemek amacıyla madde metninde değişiklik yapılması uygun görülmüştür"* denilmiştir (**Karagülmez**, s. 165).

20 **Karagülmez,** s. 20.

21 Ketizmen'de açıklamalarında *"Madde kapsamında* "girmek" *kavramı, Türkçeye "erişim" olarak çevrilen* "Access" *teriminin karşılığıdır. AKSSS'nin İngilizce metninde de bu suç* "illegal access" *(yetkisiz/hukuka aykırı erişim) olarak adlandırılmaktadır. Aynı şekilde ABD ve İngiltere'de bu suç yetkisiz erişim olarak adlandırılmakta ve bu suça ilişkin düzenlemelerde suçun maddi unsuru, sisteme erişim (access) olarak düzenlenmektedir"* demektedir (Muammer **Ketizmen**, Türk Ceza Hukukunda Bilişim Suçları, Ankara Adalet Yayınevi, 2008, s. 100).

22 Madde 2 Yasadışı Erişim:

Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezai bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar söz konusu suçu, bilgisayar verilerinin elde edilmesi amacıyla veya sahtekarlığa yönelik başka bir amaçla güvenlik sisteminin ihlal edilmesi şeklinde veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabilirler (**Avrupa Komisyonu Siber Suç Sözleşmesi Metni**, tercüme edip aktaran Ankara Barosu Siber Suç Uzmanları Komitesi, 3. Basım Ankara Barosu Yayını, Ankara 2008)

23 **Yazıcıoğlu,** "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi" s. 176, 177.

Benzer açıklamalar için bknz. B. Zakir **Avşar**/Gürsel **Öngören**, Bilişim Hukuku, İstanbul, Türkiye Bankalar Birliği Yayınları, Yayın No:270, 2010, s. 133.

AKSSS'nin 2'nci maddesinde yetkisiz erişim, kasten ve hukuka aykırı bir şekilde bir bilgisayar sisteminin tamamına veya bir kısmına girilmesi şeklinde düzenlenmiştir. Diğer bir değişle AKSSS'de sistemde kalmak aranmamıştır. Ancak söz konusu maddeye göre, yetkisiz erişim suçunu taraf devletler ceza mevzuatında düzenlerken çeşitli ek unsurlara yer verebileceklerdir. Bu ek unsurlar, güvenlik önlemlerinin ihlal edilmesi suretiyle işlenebileceği, verinin elde edilmesi ya da diğer gayri meşru bir niyetle sisteme girilmesi ya da bilgisayar ağları vasıtasıyla birbirine bağlı bilgisayar sistemleri aracılığıyla işlenebileceği şeklinde sıralanmıştır[24]. Diğer bir değişle AKSSS'nin 2'inci maddesiyle taraf devletlere mevzuatlarında, bilgisayar veri ve programlarına hukuka aykırı olarak erişimi yaptırım altına alma yükümlülüğü getirilirken, nelerin yasal olup olmayacağı konusu ile suçun oluşum koşullarını belirlemede taraf devletlere takdir yetkisi tanınmaktadır[25]. Bizim kanun koyucumuz bu noktada tercihini sistemde kalmayı da aramaktan yana kullanmıştır.

Biz makalemizde Türk ceza hukukunda hakim olan inceleme şeklinden yola çıkarak önce korunan hukuki değeri inceleyeceğiz. Ardından suçun unsurları ve suça etki eden sebeplerle suçun özel görünüş şekillerini değerlendirip, kısaca yaptırım ve soruşturma usulünü de açıklayarak incelememize son vereceğiz.

2. KORUNAN HUKUKİ DEĞER

Bilişim sistemine girme ve kalma suçuyla korunmak istenen hukuki değer[26] kanaatimizce karma niteliktedir[27]. Bu niteliklere ayrı ayrı değinmek gerekirse;

---

24 Aysun **Dalkılıç**, "Avrupa Birliğine Uyum Sürecinde Bilişim Suçları", Avrupa Birliğine Uyum Sürecinde Türk Ceza ve Ceza Muhakemesi Hukuku, Proje Yöneticisi Prof.Dr. Fatih Selami **Mahmutoğlu**, İstanbul Barosu Yayınları, İstanbul, 2008, s. 207.
Benzer açıklamalar için bknz. Şaban Cankat **Taşkın**, "Bilişim Hukuku Uluslararası Uyuşmazlıklar", Türkiye Barolar Birliği Dergisi, sayı:85, Aralık 2009, s. 334, 335.

25 Benzer açıklamalar için bknz. **Taşdemir**, s. 254; **Karagülmez**, s. 332.

26 Korunan hukuki değer, doktrinde suç tipinin ihdas edilmesi ile korunmak istenen değerdir şeklinde tanımlanmıştır (Mehmet Emin **Artuk**/Ahmet **Gökçen**/Ahmet Caner **Yenidünya,** Ceza Hukuku Özel Hükümler, 9.Basım, Ankara, Turhan Kitapevi, 2008, s. 25).

1. Toplum düzenini korumak: Maddenin düzenlendiği kısmın başlığı[28] dikkate alındığında bu amaç açıkça görülmektedir. Günümüzde tüm ekonomik ve sosyal ilişkilerin bir şekilde bilişim temelli yürüdüğü dikkate alındığında olası sistem karışıklıklarının toplum hayatını etkileyeceği kuşkusuzdur.

2. Özel hayatın gizliliği: Sistem sahibinin rızası dışında sistemine girmekle onun kişisel alanına girilmiş ve başkaları tarafından bilinmesi istenmeyen bilgileri de öğrenilmiş, dolayısıyla da Anayasa'nın 20'nci maddesinde güvence altına alınan özel hayatın korunması hakkı ihlal edilmiş olunmaktadır. Diğer bir değişle TCK'nın 243'üncü maddesiyle, bilişim sistemleri açısından Anayasa'nın 20'nci maddesi cezai anlamda güvence altına alınmıştır.

3. Haberleşmenin gizliliği: Hem çok daha hızlı olması hem de çok daha ekonomik olması nedeniyle günümüzde haberleşmede de bilişim sistemleri kullanılmaktadır. Kişiler birbirleriyle iletişim kurarken çoğu zaman, özellikle de iletişimin içeriğinden, üçüncü kişilerin haberinin olmasını istemezler. Bu nedenle sisteme yetkisiz girişler halinde haberleşme gizliliği ve özgürlüğü de etkilenmiş olacaktır. Diğer bir değişle TCK'nın 243'üncü maddesiyle, bilişim sistemleri açısından, Anayasa'nın 22'nci maddesi de cezai anlamda güvence altına alınmıştır.

4. Kullanıcı ve sistem sahibinin menfaatleri: Tüm yetkisiz girişlerin sistemin iyi çalışmadığını göstermesi nedeniyle sistem sahibinin menfaatlerine zarar verdiği gibi, verileri gözlenen kişinin de menfaatleri ihlal edilmiş

---

27 Suçla korunan hukuki değerin karma nitelikte olduğuna dair benzer görüşler ve ayrıntılı inceleme için bknz. Ahmet Caner **Yenidünya**, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu ", Legal Fikri ve Sınai Haklar Dergisi, İstanbul, Aralık 2005, Sayı:4, s. 1024; İsmail **Ergün**, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara, Adalet Yayınevi, 2008, s. 88; Şaban Cankat **Taşkın**, Bilişim Suçları, İstanbul, Beta Yayınevi, 2008, Bilişim Suçları, s. 23; Ali **Parlar**, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara, 2011, s. 15. Koray **Doğan**, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", Hukuk ve Adalet Eleştirel Hukuk Dergisi Yıl:2 Sayı:6-7, Ekim 2005, s. 294; **Taşkın**, "Bilişim Hukuku Uluslararası Uyuşmazlıklar", s. 335; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 255; **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 896,897; **Artuk/Gökçen/Yenidünya**, Ceza Hukuku Özel Hükümler, s. 682; Kurt, s. 148; Doğan **Soyaslan**, Ceza Hukuku Özel Hükümler, 8.Basım, Yetkin Yayınevi, Ankara, 2010, s. 608.

28 Maddenin yer aldığı üçüncü kısmın başlığı topluma karşı suçlardır.

olunmaktadır. Zira her giriş sistem sahibinin ve kullanıcının maddi ya da manevi zarara uğraması ihtimalini de içinde barındırmaktadır. Örneğin; bankacılık sistemlerine yetkisiz giriş halinde hem bankanın hem de bilgileri incelenen kişinin menfaatlerinin ihlal edildiği izahtan varestedir.

5. Olası başka suçların işlenmesinin önlenmesi: Sisteme giriş çoğu zaman ilk girişte olmasa dahi daha sonra başka suçların işlenebilmesi amacıyla deneme amaçlı yapılmaktadır. Bu nedenle yetkisiz girişin dahi suç olarak düzenlenmesi sonra işlenmesi düşünülen suçlara hazırlık düşüncesindeki eylemlere de engel olacaktır. Bu noktada her ne kadar TCK 243'üncü maddede sistemde kalınması da arandığından görüşümüzün hatalı olduğu akla gelebilir ise de; suç işlemek düşüncesiyle sisteme giren kişilerin zaten sistemi incelemek için kısa sürede olsa içeride kalmak zorunda olması bilişim sistemlerinde kalmanın milisaniyelerle dahi ölçülebiliyor olunması nedeniyle akla gelen bu düşünceye itibar etmiyoruz.

6. Bilişim sisteminin güvenliği: Bu suç ile bilişim sistemlerinin güvenliğinin de korunmak istenip istenmediği doktrinde tartışmalıdır. Bazı yazarlar[29] bilişim sistemlerinin güvenliğinin de korunmak istendiğini belirtirken; bazı yazarlar[30] burada bilişim sisteminin güvenliğinin korunmadığını belirtmektedir. İkinci görüşte olan yazarlar özetle TCK'nın 243'üncü maddesinde suçun oluşumu için sisteme girmenin yeterli görülmeyip sistemde kalınmasının da aranması nedeniyle sistemin güvenliğinin korunmasının söz konusu olmadığını belirtmektedirler. Bu görüşte olanlar ayrıca maddenin ikinci fıkrasında bedeli karşılığında faydalanılabilecek sitelere giriş halinde cezada indirim öngörülmüş olunmasının da görüşlerini desteklediğini belirtmekte ve burada korunan değerin kullanıcı ile sistem sahiplerinin çıkarları olduğunu belirtmektedirler. Bu noktada bizde ikinci görüşün gerekçelerini yerinde görüyoruz.

Burada kanaatimizce belirtilmesi gereken diğer bir husus maddeyle korunmak istenen değerler arasında bilişim sisteminin güvenilirliğinin de olduğudur. Ancak buradaki güvenilirlik teknik olarak güvenilirlik değildir. Yukarıda belirttiğimiz değerlerin tamamı bu güvenilirlik içerisindedir. Diğer bir değişle yukarıdaki değerlerden birinin dahi ihlal edilmesi halinde kişilerin sisteme olan güveni sarsılacak ve kişileri bilişim sistemi kullanmaktan

---

29 Örneğin bknz. Murat Volkan **Dülger**, Bilişim Suçları, Ankara, Seçkin Yayınevi, 2004, s. 214; **Doğan**, s. 294; **Taşkın,** "Bilişim Hukuku Uluslararası Uyuşmazlıklar", s. 335.

30 Örneğin bknz. **Karagülmez**, s. 166.

uzaklaştıracaktır. Dolayısıyla bilişim çağı olan günümüzde maddi ve manevi hayatımızı paylaştığımız bilişim sistemlerine güvenilirlik üst değer niteliğinde olup psikolojik bir faktör olarak görülmelidir[31].

Bu suç ile verilerin gizliliğinin de korunmak istendiği akla gelebilir ise de; kanaatimizce bu görüş yerinde değildir. Zira ileride bahsedeceğimiz üzere bazı ülkelerde bu suçun oluşumu için açıkça verilerin ele geçirilmesi düzenlenmiş iken, bizim kanunumuzda böyle bir düzenlemeye gerek görülmemiştir[32]. Kanun koyucu böyle bir koruma isteseydi, uluslararası hukuktaki durumu dikkate alarak, bunu pekâlâ açıkça düzenleyebilir ya da gerekçe de bu hususa ilişkin açıklamada bulunabilirdi.

Doktrinde bir görüş[33] ise; maddenin TBMM genel kurulundaki tartışmalarına dayanarak[34] burada aslında malvarlığına ilişkin değerlerin korunduğunu, diğer değerlerin ikinci planda kaldığını belirtmektedir. Kanaatimizce maddenin kabulü sırasında TBMM'de yapılan tartışmaların özünde

---

31 Benzer görüş için bknz. **Özbek/Doğan/Bacaksız/Tepe** s. 897; **Dülger**, Bilişim Suçları, s. 214.

32 Kişisel verilerin ele geçirilmesi ise ayrı bir suç olarak TCK'nın 136 ncı maddesinde düzenlenmiştir.

33 **Ketizmen**, s. 92 vd.

34 TCK'nın 243'üncü maddesine ilişkin TBMM Genel Kurulunda yapılan görüşmelerde madde son şeklini almıştır. Maddenin unsurlarına ve verilecek cezaya ilişkin olarak meclis görüşmeleri sırasında *"Biliyorsunuz bir de bilgisayar sistemin bozan hackerlar var, onlar size bir şey gönderdi, üzerine tıkladınız ve bir sisteme girdiniz. Hemen bunu suç haline getirirsek, çok geniş bir kapsama almış oluruz, suç kapsamını genişletmiş oluruz. Burada da -hazırladığımız taslakta- girme ve orada kalma şerhini koyduk; çünkü, bu bir kasttır. Kazara girersiniz çıkarsınız, bu başka bir şey; ama girdiniz kaldınız, değiştirdiniz, bozdunuz, bu farklı bir şey. İşte biz tasarıda, buraya açıklık getirdik. Bağlantılı olarak 244'te de bir açıklık getiriyoruz…*

Çocuğunuz 16 yaşında; geldi, bilişim sistemine girdi ve istemeden bir değişikliğe ya da veri kaybına neden oldu. Biz, şu andaki tasarıda diyoruz ki, bu kişiyi iki yıldan dört yıla kadar mahkûm edelim; ama, bir sonraki maddede diyoruz ki, bozma niyeti olana, bozma amacıyla, veriyi değiştirme amacıyla, sistemin tamamına zarar verme amacıyla bu eylemi işleyene de bir yıldan üç yıla kadar ceza verelim; hazırlanan metin bu şekilde. Şimdi, bir şey düşünün; suçu işleyen kişi, hakimin karşısına geçecek, bu işi bilmeyerek yaptıysa, daha az ceza almak için "hakim bey, benim kastım vardı, bu işi bilerek, isteyerek yaptım" diyecek ve bunun karşılığında daha az bir ceza alıp kurtulacaktı. Fiilde dengesizlik var." denilmek suretiyle değişiklik gerekçesi ileri sürülmüştür (gerekçe için bknz. **Ketizmen**, s. 98).

korunmak istenen değerin malvarlığı olduğu değil, 244'üncü maddede düzenlenen ve toplumsal güvenlik, güvenilirlik ve yukarıda saydığımız diğer değerlerin ihlalleri bakımından daha ağır olan eylemlerin cezasının 243'üncü maddeye göre daha hafif kalmasının önüne geçilmek istenmesidir. Dolayısıyla, bize göre, burada korunmak istenen değerlerden birinin de malvarlığı değerleri olduğu doğrudur (biz bunu sistem sahibinin ve kullanıcının menfaatleri başlığı altında değerlendirmeyi uygun görüyoruz) ancak bu tek veya birinci değer değildir. Korunmak istenen asıl değer yukarıda saydığımız tüm değerleri içinde barındıran sistemin güvenilirliğidir.

Sırası gelmişken belirtmek gerekir ki, TBMM Genel Kurulunda verilen önergeyle 243'üncü maddenin (1) numaralı fıkrasındaki "veya" kelimesinin "ve" şeklinde değiştirilmesi, Türk hukukunda ilk defa getirilmek istenen bu suçu, işlenmesi oldukça güç hale getirmiş ve korunmak istenilen hukuki yararı da sakatlamıştır[35].

3. SUÇUN UNSURLARI

3.1. Maddi Unsurlar

3.1.1. Fiil ve Netice

TCK'nın 243 (1)'inci maddesinde tanımlanan "bilişim sistemine girme" suçunun hareket unsuru hukuka aykırı olarak bir bilişim sisteminin bütününe veya bir kısmına girmek ve orada kalmaktır[36]. Bu suçun oluşması için icrai nitelikteki girme eyleminin ve ihmali nitelikteki sistemde kalmaya devam etme eyleminin birlikte gerçekleşmesi gerekir[37]. Kanun koyucu özel belgede sahtecilik suçunda olduğu üzere (md.207), burada da birden fazla hareketli

---

35 **Karagülmez**, s. 165.

36 Benzer açıklamalar için bknz. Nurullah **Aydın**, Türk Suç ve Ceza Hukuku Genel ve Özel Hükümler, 2. Basım, Ankara, Adalet Yayınevi, 2009, s. 382; Ali **Kiremitçioğlu**/ Taylan **Tekin**, "Bilişim Suçları ve Etkin Mücadele Yöntemleri", 14-15 Mayıs 2005 Polis Bilişim Sempozyumu, Emniyet Genel Müdürlüğü Yayını, Kataloğ No:395, s. 209; **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4631; **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 82; **Yaşar/Gökçan/Artuç,** s. 6742; **Öngören,** İnternet Hukuku, s. 46; **Dülger,** Bilişim Suçları, s. 217; **Ketizmen,** s. 81, 103; **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 901.

37 **Yaşar/Gökçan/Artuç**, s. 6743; **Ketizmen**, s. 106; **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4633.

bir suç yaratmıştır (suç, birleşik hareketlidir[38]) . Sisteme girmek yetmemekte ayrıca orada kalınmaya da devam edilmiş olunması gerekmektedir[39]. Madde gerekçesinde "girme veya orada kalmaya devam etme" fiillerinin birer seçimlik hareket olarak bu suçun maddi unsurunu oluşturacağı ifade edilmiş ise de; kanundaki açık düzenlemenin "ve" şeklinde olması karşısında bu suçta seçimlik hareket yoktur[40]. Gerekçedeki "veya" ifadesinin yasa metni gözetildiğinde hatalı olarak yazıldığını daha önce belirttiğimiz üzere TBMM genel kurulunda verilen değişiklik önergesi sonrasında "veya" ifadesinin "ve" ifadesiyle değiştirilmesine rağmen gerekçenin değiştirilmesinin unutulmasından kaynaklandığını kabul etmek doğru olacaktır[41].

Bu noktada belirtmek gerekir ki, madde başlığının "Bilişim sistemine girme" şeklinde düzenlenmesi de hatalıdır. Zira sanki suçun oluşması için sadece girmenin yeterli olduğu gibi bir kanaat uyandırmaktadır. Oysa ki, madde içeriği gereği suçun oluşması için girmek ve orada kalmaya devam etmek gerekmektedir. Bu nedenle maddenin başlığının düzeltilmesi gerektiğini düşünmekteyiz[42]. Ayrıca belirtmeliyiz ki, doktrinde TCK'nın "hukuka aykırı erişimi" suçun oluşması bakımından yeterli saymaması eleştiri konusu olmaktadır[43].

Failin, sisteme kendi adına ya da bir başkası adına girmesi de suçun oluşmasını önlemeyecektir[44].

---

38 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4633; **Özbek/Doğan/ Bacaksız/Tepe**, s. 903.

39 İsmail **Malkoç**, "Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu", Ankara, Malkoç Kitabevi, 2. Cilt, 2007, s. 1668; İnci **Biçkin,** "Siber Suç Sözleşmesi ve 5237 s. Türk Ceza Kanununda Bilişim Suçları", Yargıtay Dergisi, Cilt:32, Ocak-Nisan 2006, Sayı:1-2, s. 152; **Yazıcıoğlu**, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 82; **Kurt,** s. 147; **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4633.

40 Sinan **Esen**, Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanındaki Suçlar, Ankara, Adalet Yayınevi, 2007, s. 628; **Dalkılıç,** s. 218.

41 Ali **Parlar**, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara, 2011, s. 16; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 257; **Esen,** s. 62; **Doğan,** s. 295.

42 Benzer açıklamalar için bknz. **Karagülmez**, s. 169.

43 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4632.

44 **Taşkın,** "Bilişim Hukuku Uluslararası Uyuşmazlıklar", s. 336.

Girme ve orada kalma hareketi bilişim sistemi aracının bazı parçalarının açılarak veya çıkarılarak bilişim sistemi aracının içine fziken girilmesi anlamında değildir. Çalışan bilişim sistemi aracının sanal alanının içine girmedir. Bilişim sistemi aracı çalışmakta ve fail başkalarına ait verilere vakıf olabilmektedir[45]. Diğer bir değişle, girmek kavramı bilişim sisteminin yazılımla ilgili bölümünün tamamına veya bir kısmına ulaşmak, dahil olmak, erişmek anlamına gelmektedir. Bu suç, bir kimsenin emanet ettiği 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. Örneğin; bir bankanın hesaplarına girilerek müşteri hesabına hukuka aykırı olarak bakılması[46] veya bir kamu kurumunun bilgisayarına dışarıdan hukuka aykırı olarak girerek orada belli bilgilerin incelenmesi veya birisinin açık bilgisayarında belli pencerelerin açılarak bakılması eylemi anılan suçu oluşturacaktır. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden bu durum girme kapsamında düşünülemez[47]. Ancak burada belirtmeliyiz ki şayet e-posta sıradan bir e-posta olmayıp casus program barındırıyorsa, artık suçun icra hareketlerinin başladığını kabul etmemiz gerekir. Zira e-posta açıldığında casus program

---

Yargıtay 11. CD. 24.9.2010, 10299-9933 esas ve karar sayılı ilamında özetle "*Sanığın Halley ınternet Cafe'nin sahibi olduğu, iş yerindeki 70 adet bilgisayarın "gözetimi ve denetimi için gerekli hassasiyeti göstermemesi sebebiyle kusurlu olduğu gerekçesiyle cezalandırılmasına karar verilmiş ise de, adı geçen iş yerindeki İP numarası 81.215.188.170 olan bilgisayardan müştekinin elektronik posta adresine girilmesinden sanığın sorumluluğu olmamasına rağmen, üzerine atılı suçtan beraatine dair karar verilmesi gerekirken yazılı şekilde cezalandırılmasında..."* demektedir (**Parlar,** s. 19).

45 **Soyaslan,** s. 609.

46 Sanığın, katılanın yetkilisi olduğu Z... Tekstil Şirketinin T. E. Bankası D.. 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 s. TCK'nın 243 (1) maddesinde düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde (5237 s. TCK'nın 244(4), 35/(2) maddeleri gereğince hüküm tesisi… (11. CD'nin 26.03.2009 tarih ve 18190-3058 sayılı kararı) aktaran, **Yaşar/Gökçan/Artuç**, s. 6744.

47 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4631.

harekete geçecek ve sistem içerisinde gizlenip failin amaçlarına hizmet edecektir[48].

TCK'nın 243'üncü maddesinde sistemin bir kısmına veya tümüne girmek arasında bir fark görülmemiştir. Diğer bir değişle, suçun oluşumu için sistemin tümüne girmek şart değildir. Sistemin bir bölümüne girmekle de suç oluşacaktır[49]. Sistemin bir kısmından maksadın ne olduğu ise, yasa metninde ve gerekçesinde açıklanmamıştır. AKSSS Taslağı ve Açıklayıcı Memorandumu'na bakılarak bilişim sisteminin, donanım, bileşenler, yüklenen sistemin saklanan verileri, dizinler, trafik ve içerikle ilişkili veriler gibi unsurlarından bir yahut birkaçına girilmesinin gerektiği doktrinde ileri sürülmüş ise de[50]; kanaatimizce donanım kısmına giriş yapmak mümkün değildir. Bilişim sisteminin sanal alanına girilmelidir. Ancak bu giriş fiziki temasla da gerçekleştirilebilir[51].

Bilişim sisteminde "kalmaya devam edilmesi" kavramından ne anlaşılmalıdır? Yasa koyucu burada yasal düzenlemeyi yaparken ne metinde ne de gerekçede bu hususa değinmemiştir. Öncelikle belirtmek gerekir ki fiilin gerçekleşmesi için bilişim sisteminde kalınan süre konusunda kesin bir kıstas koymak zordur.

Bir görüşe göre[52], her girme eylemi aslında kalma eylemini de zorunlu olarak içermektedir. Çoğunlukla girmekle birlikte yani güvenlik duvarının

---

48 Benzer görüş için bknz. **Taşkın,** "Bilişim Hukuku Uluslararası Uyuşmazlıklar", s. 335.

49 Benzer açıklamalar için bknz. Ö. Umut **Eker**, "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:19, Sayı: 62, Ocak-Şubat 2006, s. 123; Ali **Kiremitçioğlu**/Taylan **Tekin**, "Bilişim Suçları ve Etkin Mücadele Yöntemleri", 14-15 Mayıs 2005 Polis Bilişim Sempozyumu, Emniyet Genel Müdürlüğü Yayını, Kataloğ No:395, 2005, s. 209; **Taşkın,** Bilişim Suçları, s. 25; **Taşkın,** "Bilişim Hukuku Uluslararası Uyuşmazlıklar", s. 335; **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 82; **Malkoç,** s. 1669; S**oyaslan,** s. 609.

50 **Eker,** s. 123.

51 Benzer açıklamalar için bknz. **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçlarıs. 258; **Yazıcıoğlu,** "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi" s. 176,177.

52 Giriş yapıldığı anda suçun da oluştuğunu kabul etmek gerektiği görüşü için bknz. **Özbek/Kanbur/Doğan/Bacaksız/Tepe,** s. 902; **Yazıcıoğlu**, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 83; **Soyaslan**, s. 608.

aşılması ile birlikte zaman mefhumu olmaksızın kalma eylemi de başlamış olmaktadır; zira suç zorunlu olarak bir mütemadi suçtur. Ayrıca bir milisaniyede bile olsa verileri elde etme olanağı bulunduğu için kalma zorunlu olarak gerçekleşmiş olacaktır.

Diğer görüş ise[53], kişinin bir bilişim sistemine girdiğini anlamasına rağmen sistemi terk etmemesi halinde suçun tamamlandığını, bilişim sistemine girdikten sonra hemen çıkılırsa (mümkün olan en kısa zamanda) suç oluşmayacağını; zira maddenin sisteme giren ve orada kalmaya devam eden kimsenin fiilini yaptırım altına aldığını, bu suç ile sistem sahibinin özel alanının masuniyeti, huzur ve sükunu, verilerinin gizliliğinin korunmak istendiğini, bu nedenle belirtilen değerleri ihlal edebilecek kadar bilişim sistemi içerisinde kalmış olmanın suçun oluşumu için yeterli kabul edileceğini belirtmiştir. Bu görüşün taraftarları sürenin her olayın koşullarına göre ayrı olarak belirlenmesi gerektiğini, hakimin bu konuda takdir yetkisini kullanması gerektiğini söylerler. Örneğin; bilişim sistemine giren ve orada 3-5 dakika kadar kalan ve daha sonra sistemden çıkan bir failin mahkemede yaptığı savunmasında, bilişim sistemine sırf merak saikıyla ve başarabilir miyim düşüncesiyle girdiğini, sonra da bunu başarınca sistemde çok beklemeden ayrıldığını söylemesi halinde, bu kadar kısa süreli bir girişin savunmayı destekler mahiyette olduğu düşünülerek sadece bu suça teşebbüsten hüküm kurulabileceğini, ancak yine de, her olayın durumuna göre ne sürede sistem içerisinde kalmanın suç işleme kararını göstereceğine ve suçun tamamlanmış sayılacağına hakimin karar vereceğini belirtirler. Bu görüş taraftarlarından Pallı ayrıca Çince bilmeyen bir Türk, Çin'de faaliyet gösteren bir firmanın bilgisayar sistemine yalnızca becerisini kanıtlamak için girmesi halinde pek çok saat de sistemde kalsa oradaki bilgileri öğrenemeyeceğinden suçun düzenleniş amacının ihlal edilmiş olunmayacağını da söylemektedir[54].

Biz iki görüşe de doğrudan katılmıyoruz; kanaatimizce failin bilişim sistemine eriştiğini öğrendiği anda sistemden hemen çıkmamış olması suçun tamamlanması için yeterlidir. Zira bu durumda suçla korunan hukuki yarar-

---

53 **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 257-259; **Yaşar/Gökçan/Artuç**, s. 6743; **Kurt**, s. 154; **Pallı,** s. 156, 157; **Yenidünya,** s. 1034.

54 **Pallı,** s. 156, 157.

ların tümü ihlal edilmiş olunmaktadır. Biz suçun oluşumu için bilgileri öğrenmenin aranmaması nedeniyle ikinci görüşe doğrudan katılmıyoruz. Çince hazırlanan siteye ilişkin örneği ise, sitede kişilerin özel fotoğraflarının ya da görsel faktörlerinin bulunması ihtimalinin de bulunması, kaldı ki Çince'de olsa siteye girmekle toplumsal güvenilirliğin zedelenmiş olması nedeniyle uygun bulmuyoruz. Biz ilk görüşe de doğrudan katılmıyoruz; çünkü bu görüşün doğrudan kabulü halinde kanun metnindeki "kalmaya devam etme" unsuru anlamsızlaşmaktadır[55]. Ayrıca unutulmamalıdır ki, "Kalmaya devam etme" olgusundaki zaman dilimi, bilişim alanında ileri düzeyde bilgi ve beceriye sahip olan bir fail için kısa olabilirken, daha az bilgi ve beceriye sahip olan fail bakımından daha uzun olabilecektir[56].

Kanun koyucu burada serbest hareketli bir suç düzenlemektedir; yani suçu meydana getiren hareketi tanımlamayarak girme ve sistemde kalmaya yarayacak her fiili, yöntemi ne olursa olsun[57], madde kapsamı içine almış

---

55 Benzer görüş için bknz. **Karagülmez,** s. 170; **Artuk/Gökçen/Yenidünya,** Türk Ceza Kanunu Şerhi, s. 4632.

56 **Karagülmez,** s. 170.

57 Bir bilişim sistemine başka bir sistem yoluyla girmenin en temel iki yöntemi bulunmaktadır:

1.Mevcut Açıklardan Yararlanmak*;* bilişim alanına zarar verilmesi konusunda olduğu gibi girilmek istenen sistemde bulunan bir açığı değerlendirmektir. Sisteme girmek isteyen kişi, çeşitli metotlarla herhangi bir ağa (mesela internete veya şirket içi bilgisayar ağına) bağlı bulunan bir bilgisayarın zayıf noktasını bulmaya çalışır ve genel ya da özel kast ile aradığı kurban makinenin açığını yakaladığında, yine sıradan kullanıcıların pek aşina olmadığı yöntemlerle o sisteme girer. Yani, bu yöntemde failler sistemlere haksız erişim sağlamak için girmelerini sağlayacak bir ön zarar vermemekte, mevcut eksikliklerden istifade etmektedirler.

2.Açık Sağlayarak Sisteme Girmek*;* açık sağlayarak sisteme girmek kavramından kasıt, ağa bağlı bir bilişim sistemine karşı yukarıda izah ettiğimiz girme fiilini gerçekleştirmek için sıradan bir makine olarak güvenlik eksikliği bulunmayan cihazda açıklar meydana getirecek eylemlerde bulunduktan sonra sisteme sızmaktır. Yani, fail bu kez mevcut bir açığı değerlendirmeyecek, önce hedefindeki sistemi sızabilir hale getirip ardından uzaktan girişi sağlayacaktır. Bu ihlali gerçekleştirmenin en yaygın yöntemi ise Truva Atı (Trojan Horse) denilen programları kullanmaktır (Hatice **Akıncı/**A. Emre **Alıç/**Cüneyd **Er**, "TCK ve Bilişim Suçları", İnternet ve Hukuk (Derleyen Yeşim M. A. **Tamer**), İst. Bilgi Ünv. Yayınları, s. 175, 176.

Hackerlerin izlediği yola baktığımızda; hackerların önce hedef belirlemesi yaptıklarını, zarar verecekleri veya elde edecekleri sistemi belirlediklerini tespit etmekteyiz. İkinci etapta, o sistemle, bilgisayarla ilgili bilgi toplamaya başlanmakta; örneğin IP aralıklarını

bulunmaktadır. Her türlü hareket ile bu suç gerçekleştirilebilir; yeter ki sistemin yazılımsal yanına girme ve orada kalma eylemi gerçekleşiyor olsun. Giriş kablolu, kablosuz bağlantı ile olabileceği gibi kızılötesi ışınlar[58] ile de olabilir; hatta bluetooth[59] gibi sistemler marifetiyle veya manuel olarak yani doğrudan bir bilişim sistemi ile fiziki temasa geçerek sistemi kullanmak suretiyle sisteme girmek şeklinde de cereyan edebilir[60].

---

taramakta, fire wall var mı veya fire wall açıkları nelerdir, neler değildir? şeklinde birtakım bilgiler derlenmektedir. Bu toplanılan bilgiden hareketle araçlar hazırlanmakta, yani nasıl, nereye saldırılacağı ve nereden müdahale edilebileceği saptanmaktadır. Daha sonra bu araçla birlikte nüfuz etme yöntemi başlamaktadır. Son olarak da yapılan işlemlerin izlerini silme aşaması söz konusudur. Ülkemizde bu konuyla ilgili şu ana kadar tespit ettiğimiz, yakaladığımız ve işlem yaptığımız hackerlerın bu kadar profesyonel olduklarını söylemek mümkün değildir. Genel olarak aynı süreç takip edilmesine rağmen sadece son maddedeki izleri silme uygulamasının ülkemizdeki hacker olarak tabir ettiğimiz kişiler tarafından yapılmadığı tespit edilmiştir. Bu işi yapan en profesyonel hackerler, önce sisteme girmekte ve sonra sistem içindeki tüm izleri yok etmektedirler. Çünkü emniyet birimleri bu kişileri o izleri takip ederek bulabilmektedir (Ayhan **Çankaya**, "Bilişim Suçlarıyla Mücadelede Gelinen Durum", Bilişim Hukuku, İstanbul, Kadir Has Üniversitesi Yayınları, Derleyen Mete **Tevetoğlu**, 2006, s. 93, 94).

58 Görülebilen kırmızı ışıktan daha uzun dalga boyuna sahip, gözle görülmeyen ışınların veri iletilmesinde kullanılmasını sağlayan aygıtlardır. Uzaktan kumanda aletleri, bilgisayarlar ile el bilgisayarları (PDA), mobil telefonlar arasında veri iletimi için kullanılmaktadırlar (Burak **Çekiç**, İnternet Aracılığıyla İşlenen Suçlar, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Anabilim Dalı, Kamu Hukuku Bilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2006, s. 19).

59 Kablo bağlantısını ortadan kaldıran kısa mesafe radyo frekansı teknolojisinin adıdır (Eralp, s. 34). Bluetooth, Ericson firması tarafından 1994 yılında cep telefonları ve diğer mobil cihazları kablosuz olarak birbirine bağlayabilmek ve iletişim kurabilmek için geliştirilmiştir (http://tr.wikipedia.org/wiki/Bluetooth 19.03.2010).

Bugün pek çok insanın kullandığı televizyonların uzaktan kumandası, aslında Bluetooth'un atası sayılabilir. Ancak aradaki en büyük fark, şu an kullanılmakta olan uzaktan kumandalar (TV vb.), IrDA (infra Red Data Association), kızıl ötesi ışık ile veri iletişimini sağlamaktadır. Bluetooth'da ise 2.4 GHz'de radyo dalgaları kullanılmaktadır. Bunun sonucunda ise, IrDA gibi doğrudan görüş hattı gerektirmemenin üstünlüğünü sunmaktadır (http://www.wifi-turk.com/makale-8-wi-fi-nedir-ve-bluetooth-arasindaki-farklar.html 19.03.2010).

60 **Yenidünya,** s. 1035; **Kurt,** s. 156; Esen, s. 629; **Dülger,** Bilişim Suçları, s. 217, 218; **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 83, 84; **Taşdemir**, Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 256, 257; **Taşkın**, "Bilişim Hukuku

Bu suçun işlenebilmesi için söz konusu sisteme bir şifre veya kullanıcı adı vasıtasıyla erişilebiliyor olması şart değildir. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows,linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de pekala bu suçu oluşturacaktır[61]. O halde büyük bir bilgisayarın içine girip orada geceleyen kimsenin eylemi bu suç kapsamında değerlendirilmeyecektir[62]. Ayrıca mağdur tarafından açılan bir dosyanın başkaları tarafından görülmesi halinde (örneğin, monitörden) bilişim sistemine girme söz konusu değildir. Çünkü fail tarafından sisteme herhangi bir müdahalede bulunulmamaktadır. Ancak mağdurun çalışır halde bıraktığı bilgisayarında kayıtlı bulunan bir dosyayı, klavye veya fareyi kullanarak açan ve içeriğine nüfuz eden kimsenin eylemi 243'üncü madde kapsamında değerlendirilir[63].

Ayrıca fail sisteme hukuka uygun olarak girip izni bittikten sonra hukuka aykırı olarak kalmaya devam ederse ne olacaktır? Yasanın gösterdiği birinci hareket yapılmadığı için suç oluşmayacak mıdır? Kanaatimizce Kanun metninde hukuka aykırı olarak girme ve orada kalmaya devam etme unsurları açıkça arandığı için hukuka uygun girdikten sonra hukuka aykırı olarak orada kalmaya devam edilmesi halinde suç oluşmayacaktır. Aksinin kabulü "suçta ve cezada kanunilik ilkesi" gereği mümkün değildir[64]. Ayrıca belirtmeliyiz ki, kanun koyucu sanal ortama yetkisiz girişin somut hayatta karşılığını oluşturan konut dokunulmazlığını ihlal suçunu 116'ncı maddede düzenlerken açıkça "rıza ile girdikten sonra buradan çıkmayan kişi" ifadesini kullanmışken, sanal alan için böyle bir ifadeye yer vermemesi de görüşümüzü güçlendirmektedir.

Burada incelenmesi gereken diğer husus, genel olarak bilişim sisteminin bütününe ya da bir kısmına girmeye yetkili olan bir kişinin sisteme

---

Uluslararası Uyuşmazlıklar", s. 335; **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 903; **Kiremitçioğlu/Tekin**, s. 209.

61 **Doğan**, s. 296. Benzer açıklamalar için bknz. **Yenidünya**, s. 1035; **Taşkın,** "Bilişim Hukuku Uluslararası Uyuşmazlıklar", s. 335.

62 **Yaşar/Gökçan/Artuç**, s. 6742.

63 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4635.

64 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4635; **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 82, 83; **Taşdemir**, Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 256; **Yaşar/Gökçan/Artuç**, s. 6743; **Ketizmen,** s. 107.

kendisine ait oturum açma yetkisinin ilişkilendirildiği kullanıcı hesabından başka bir hesap ile sisteme girmesi olasılığıdır. Burada özellikle iki olasılık açısından değerlendirme yapılması gerekir. Bunlardan birincisi, sistem içerisinde işlem yapma yetkisinin kapsamı, diğeri ise maddede açıkça vurgulandığı üzere, bilişim sistemi içerisinde sistemin belirli kısımlarına girişe ilişkin yetkilendirme olarak karşımıza çıkmaktadır[65].

TCK'nın 243'üncü maddesindeki suç sistem içerisinde işlem yapma yetkisinin kapsamı bakımından incelendiğinde; doktrinde[66] yetki derecesine göre ayrım yapılmaktaysa da; kanaatimizce ne şekilde olursa olsun suç maddi unsurlar bakımından oluşur. Zira neticede kendisine ait şifre ve alanını kullanabilecekken başkasının şifre ve alanını kullanmıştır. Kaldı ki bilişim sisteminin soyutluğu ile sistemin sonsuz büyüklüğü dikkate alındığında failin başkasının şifresiyle ya da başkasının alanında ne yaptığının özel çaba sarf etmeden tespit imkanı da yoktur. Ancak manevi unsur bakımından değerlendirmede somut olayın özelliklerine göre suç oluşmayabilecektir.

Yukarıda anlattıklarımızı özetletmek gerekirse, bir bilişim sistemine hukuka aykırı olarak girmenin TCK m. 243 (1)'de düzenlenen suça vücut verebilmesi için asgari olarak şu iki unsuru içinde bulundurulması gerekir[67]:

- Her şeyden önce söz konusu bilişim sistemine erişimin bir takım tedbir veya uygulamalarla sınırlandırılmış olması gerekmektedir. Burada sınırlandırmadan kastedilen şey, bilişim sisteminin işleyişinin ancak işlem yapma yetkisine sahip kişilerce gerçekleştirilebilmesidir. Böyle bir yetkilendirmeye en bariz örnek, şifrelendirilmiş bilişim sistemlerindir. Bu tür bilişim sistemlerine erişim ancak daha önce tespit edilmiş ve sadece belli kişiler tarafından bilinen bir şifre ile mümkün olabilmektedir. Dolayısıyla herkes tarafından arzu edildiği her an erişilebilen bilişim sistemleri (örneğin; herkesin kullanımına açık internet siteleri) TCK m. 243 (1)'in konusunu teşkil etmemektedir.

- Erişimi mümkün kılacak yetkinin usulüne uygun olarak alınmış olması gerekmektedir. Bu noktada gerekli yetkinin alınmasında hangi usule riayet edileceği, o bilişim sistemine erişimi sınırlayan yönetici birim tarafın-

---

65 **Ketizmen,** s. 104.

66 **Ketizmen,** s. 104. Benzer açıklamalar için bknz. **Dalkılıç,** s. 219.

67 **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 900.

dan belirlenmektedir. Belirlenen prosedür ve kurallar dışında erişim için gerekli unsurlar temin edilmiş olsa bile usulüne uygun bir yetkilenme gerçekleşmediği için yetkisiz erişim söz konusu olacaktır. Ayrıca, usulüne uygun alınmış bir kullanıcı adı ve şifresinin bir başka kişi tarafından sahibinin rızası hilafına hukuka aykırı bir şekilde temin edilmesi ve bu suretle erişimin sağlanması durumunda da yetkisiz erişimin gerçekleştiği kabul edilmelidir.

Birçok ulusal mevzuatta yetkisiz giriş suçlarıyla ilgili hükümler bulunmaktadır; ancak suçun kapsamı ve unsurları önemli ölçüde farklılık göstermektedir.

Bilişim suçları için öngörülen eylemler bakımından 1994 tarihli Yeni Fransız Ceza Kanunu (m.323.1/1)[68], 88-19 sayılı Kanunla değişik eski Fransız CK. (m.462.2/1)[69], Lüksemburg CK. (m.509.1/1)[70], Norveç CK.

---

68 Yeni Fransız CK. m.323.1/1: *"Verileri otomatik işleme tabi tutmuş bir sistemin tamamına veya bir kısmına hileyle (hukuka aykırı olarak) girme veya burada kalma fiili bir sene hapis ve 100.000 Frank para cezasıyla cezalandırılır"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 76.

Fransız Ceza Kanununun 323'ncü maddesi incelendiğinde sırf otomatik bilişim sistemine tamamen veya kısmen haksız biçimde girmenin suç olarak düzenlediği, bunun dışında girilen sisteme kaydedilmiş verileri silme, değiştirme veya sistemin fonksiyonlarını değiştirme hallerininse, 3'üncü fıkrada, cezayı ağırlatıcı neden olarak düzenlendiği görülmektedir (**Ünver,** "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının (2000) İnternet Açısından Değerlendirilmesi", s. 71).

69 Kanunun 462.2 nci maddesi: *"Her kim, hukuka aykırı olarak otomatik işleme tabi kılmış bir sistemin tamamına veya bir kısmına girer veya burada kalırsa iki aydan bir yıla kadar hapis ve 2 000 franktan 50 000 franka kadar para cezası ile veya iki cezadan birisi ile cezalandırılır.*

Bu hareket sistemdeki verilerin değişmesine veya yok olmasına, sistemin işleyişinde bir değişikliğe sebebiyet verirse, hapis cezası iki aydan iki yıla kadar ve para cezası 10 000 franktan 100 000 franka kadardır" (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 76).

70 Lüksemburg CK. m.509.1/1: *"Her kim, verileri otomatik işleme tabi tutmuş bir sistemin tamamına veya bir kısmına hileyle (hukuka aykırı olarak) girer veya kalırsa iki aydan bir seneye kadar hapis ve 10.000 Franktan 250.000 Franka kadar para cezasıyla veya bu iki cezadan birisiyle cezalandırılır"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 76).

(m.145/2)[71], 1973 tarihli ve 283 sayılı İsveç Data Protection Act (m.21)[72], 27 Aralık 1991 tarihli İrlanda Criminal Damage Act (m.5 (1) a. ve b.)[73], 17 Ağustos 1991 tarihli ve 91/109 sayılı Portekiz Bilgisayar Suçları Hakkında Kanun (m.7)[74], Yunan CK. (m.370 C/2)[75], 1990 tarihli İngiliz Computer Misuse Act (m.1)[76], Hollanda FK. (m.138a)[77], İtalyan CK. (m.615-ter)[78],

---

71 Norveç CK. m.145/2: *"Her kim, bir password veya kodu berteraf ederek, elektronik veya diğer teknik usullerle depolanan veya ulaşılan veri veya yazılıma hukuka aykırı olarak girerse yukarıdaki fıkrada öngörülen cezayla (altı aydan az olmamak üzere hapis cezasıyla) cezalandırılır"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 76).

72 İsveç Verileri Koruma Hakkında Kanun m. 21: *"Her kim, bilgileri otomatik işleme tabi tutmuş bir sistemdeki verilere hukuka aykırı olarak ulaşır veya bunlara bir giriş elde ederse ... fiil ayrı bir suç oluşturmadığı takdirde ceza kanundaki mala zarar verme suçuna ait cezayla birlikte ağır para cezası veya iki yıla kadar hürriyeti bağlayıcı cezayla cezalandırılır"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 76).

73 İrlanda Criminal Damage Act m.5 (1) a.: "*Her kim meşru bir sebep olmaksızın bir bilgisayar sistemine: (a) kasten ülke içinden ülkede veya dışında yer alan bir veriye giriş yaparsa; (b) kasten ülke dışından, ülkede yer alan bir veriye giriş yaparsa ..."* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 76).

74 Bilgisayar Suçları Hakkında Portekiz Kanunu m.7: *"Her kim, yetkisiz olarak ... bir menfaat veya hukuka aykırı bir yarar elde etmek için her ne suretle olursa olsun bir sisteme veya bilişim ağına girerse bir seneye kadar hapis veya yüzyirmi gün birimlik para cezasıyla cezalandırılır"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 76).

75 Yunan CK. m.370.C/2: *"Her kim, meşru bir hakkı olmaksızın hak sahibinin rızası hilafına veya almış olduğu emniyet tedbirlerini bertaraf ederek bir bilgisayarda veya bu bilgisayarın hafızasında yer alan veya bir telekomünikasyon sistemiyle aktarılan verilere girerse üç aya kadar hapis cezası veya 10.000 drahmiye kadar para cezasıyla cezalandırılır. Eğer bu fiil, Devletin güvenliğini veya uluslararası ilişkilerini tehlikeye sokarsa m.148'deki cezalar tatbik olunur "* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 76).

76 Kanunun 1.kısım: (*Unauthorised access to computer material*) Bilgisayarlardaki veri ve programlara yetkisiz olarak girilmesini; 1.-(1)(a) Bilgisayarlarda yer alan veri veya programlara girebilmek amacıyla bunlara müdahale edilmesini;

(b) yetkisiz olarak girilmesini ve

(c) yukarıda belirtilen eylemlerin gerçekleştirildiği sırada failin bu müdahalenin gayrimeşru olduğunun bilincinde olmasını;

(2) bu müdahalenin doğrudan:

(a) özel bir program veya veriye;

(b) Kendine has bir program veya veriye;

(c) özel bir bilgisayardaki bir program veya veriye karşı işlenmesi" halinde suç olarak düzenlemekte ve 1'inci kısım 3'üncü madde ile de altı aya kadar hapis veya belli bir miktar para cezasıyla cezalandırmaktadır (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 77). Bu kanunla "yetkisiz olarak bilgisayarlara girilmesinin veya değişiklik yapılmasının veyahut benzeri müdahalelerde bulunulmasının önlenmesi" amaçlanmıştır. Bu kanunla temel olarak üç tür suç tipi belirlenmiştir (**Akıncı/Alıç/Er,** s. 202). İngiltere'de bu Kanunun birinci bölümü hack ve buna bağlı elementleri suç sayar: Kanunun 17(5) bölümü derki; herhangi bir programa veya veriye herhangi bir insan tarafından yapılan her çeşit erişim, eğer söz konusu programa veya veriye erişimi kontrol etmekle vazifeli değilse ve herhangi bir yetkili kişi tarafından söz konusu programa veya veriye erişim iznine sahip değilse yetkisizdir. Yetkili kullanıcıların kasıtlı olarak yetkilerini aşması da yetkisiz erişim kapsamına girer (Sandra **Mariana**, Cyber Crime: a Comparative Law Analysis, http://uir.unisa.ac.za/bitstream/10500/2056/17/03chapter3.pdf 21.07.2010). Dikkat edilirse sadece erişim de suç sayılmaktadır. Buna göre basit bir meraktan veya güvenlik sistemini denemek amacıyla işletim sisteminin güvenliğini kırmak için tasarlanmış tüm faaliyetler zarar kastı taşısın ya da taşımasın yasadışı sayılacaktır. Sorumluluk için tek ön şart failin, girişinin yetkisiz olduğunun bilincinde olmasıdır (**Wikipedia**, The Free Encyclopedia; http://en.wikipedia.org/wiki/Computer_Misuse_ Act_1990, 08.08.2007, tercüme edip aktaran, **Pallı**, s. 112, 113).

"The Police and Justice Act 2006" isimli Kasım 2006'da yürürlüğe giren yasanın 48'inci kısmı, "The Computer Misuse Act 1990" üzerinde değişiklikler yapmıştır. Bilgisayar materyallerine yetkisiz giriş suçunda eylemin kapsam alanı genişletilmiş, bilgisayar materyallerinde yetkisiz değişiklik yapmak suçu kaldırılarak yerine bilgisayar ve sairenin işletimini bozmak kastıyla veya dikkatsizlikle yapılan yetkisiz eylemler de suç sayılmıştır (**Pallı,** s. 112, 113).

77 Hollanda CK. md 138a/1: *"Her kim kasten ve hukuka aykırı olarak verileri otomatik işleme tabi tutan veya saklayan bir sisteme girerse ... altı aya kadar hapis veya 100.000 Florin para cezasıyla cezalandırılır"* tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 77).

78 İtalyan CK. m.615-ter: *"Her kim emniyet tedbirleri ile korunan bilişim veya telematik bir sisteme hukuka aykırı olarak girer veyahut böyle bir sistemde oradan çıkarma hakkına sahip bir kimsenin açık veya zimni rızası hilafına kalırsa üç seneye kadar ağır hapis cezasıyla cezalandırılır.*

1) Eğer fiil, bir C. Savcısı veya kamu hizmetlisi tarafından yetkilerini kötüye kullanarak veya vazifesi veya hizmetine ilişkin görevini suistimal ederek veya hususi olarak soruşturma işleriyle iştigal edip de mesleğini ihlal eden veya sistem operatörlüğü görevini suistimal eden kimse tarafından işlenirse;

İsviçre CK. (m.143-*bis*)[79] gibi bazı kanunlar, sadece hukuka aykırı (yetkisiz) olarak bir bilgisayar veya sistemine yahut buna ilişkin program ve verilere girilmesini yaptırım altına alırken; Yunan CK. (m.370 B ve 370 C/1), Kanada CK. (m.301.2(1)a ve c), Hollanda CK. (m.139a), Finlandiya CK. (28. kısım m.7,8,9) gibi bazı kanunlar ise hukuka aykırı (yetkisiz) olarak bunların kullanılmasını da suç haline getirmektedirler. Yukarıdaki düzenlemelerin yanında bazı devletlerde, resmi nitelikli bilgisayarlara (örneğin; Avustralya CK. m.76 B (1)a.) siyasi veya devlet sırrına ilişkin bilgilere ulaşmak (örneğin; ABD[80] 18 USC -United States Code- 1030 uncu kısım

---

2) Eğer fail, suçu işlemek için aşikar bir silah veya eşya veya şahıslar üzerinde cebir kullanırsa;

3) Eğer fiil, sisteme zarar verir veya tahrip ederse yahut kısmen veya tamamen işlemesine engel olursa veyahut buralardaki veri, bilgi veya programlara zarar verir veya tahrip ederse;

Ceza bir seneden beş seneye kadar ağır hapis cezasıdır. (...) (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 77).

İtalyan Ceza Kanunu'nun 615ter maddesi, 765 s. Türk Ceza Kanunu'nda bulunmamakta ise de, 5237 s. Türk Ceza Kanunu'nun 243'üncü maddesindeki "Bilişim sistemine girme" suçuna benzer gözükmektedir. Ancak, 615 ter maddesindeki, bilişim sistemine hukuka aykırı girme veya haksız yere sistemde kalmaya devam etme seçimlik hareket şeklindedir ve yalnızca girme fiili de bu suçu oluşturmaktadır. Oysa 5237 s. Türk Ceza Kanunu'nda, "girme" hareketi 243'üncü maddedeki suçun oluşumu için yeterli olmadığı gibi teşebbüs için yeterli olup olmadığı da, ileride açıklanacağı üzere tartışmalıdır. Ayrıca 615ter maddesi, güvenlik önlemleriyle korunan bilişim veya telematik sistemine hukuka aykırı şekilde girme veya böyle bir sistemde rıza göstermeye yetkili kişinin rızası olmaksızın kalma fiilini suç olarak düzenlemiştir. (**Karagülmez,** s. 103).

79 İsviçre CK. M.143-bis: *"Her kim, veri nakline yarayan bir aygıt ile başkalarının girişine karşı korunan bir bilişim sistemine zenginleşme amacı olmaksızın yetkisiz olarak girerse, şikayet halinde hapis veya para cezasıyla cezalandırılır".* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 77).

80 1984 yılında Amerikan Kongresi "Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Yasası"nı ülke çapında artan "hacking" eylemlerine çare olarak kabul etmiştir. Bu yasa ile Federal Temel Yasa'nın 18 nci Bölümünün 1030 ncu maddesi değiştirilmiştir. (18 U.S.C. § 1030). Başlangıçta yasanın kısa ve dar ölçekli olması amaçlanmıştır. Ancak, günden güne artan ve bilgisayar güvenliğini tehdit eden eylemler sonucunda, çeşitli değişiklikler yapılmıştır. Yasa temel olarak, korumalı bir bilgisayara yetkisiz ve izinsiz erişimi yasaklamaktadır. Yasa metni o kadar geniş kaleme alınmıştır

a)(1)) yahut finans dünyasına ilişkin konularda bilgi edinmek (örneğin, USC 1030 uncu kısım a) (2)) amacıyla yetkisiz olarak girilmesini suç haline getirmektedir[81].

---

ki, kamuya ve özel sektöre ait tüm bilgisayarlar yanında, kişisel bilgisayarlar da bu korumadan tam olarak istifade edebilmektedir.

Bu yasa ile suç haline sokulan hareketler şunlardır:

ABD hükümetine zarar vermek veya herhangi bir yabancı ülkeye yarar sağlamak maskadıyla, tasnif edilmiş ve gizlilik dereceli savunma ve dış işleri konularına ilişkin enformasyona izinsiz olarak erişmek,

Finansal bir kurum veya tüketici araştırma ajanslarından herhangi birinin bilgisayarlarındaki finansal kayıtlara izinsiz ve yetkisiz olarak erişmek,

Kamu kuruluşlarından herhangi birinin kullandığı bir bilgisayara girerek, bu kuruluşların verdiği hizmeti aksatacak şekilde, burada bulunan bilgileri değiştirmek, bozmak veya ifşa etmek

Herhangi bir bilgisayara sahtekarlık veya hırsızlık yapmak maksadıyla izinsiz ve yetkisiz olarak girmek,

Herhangi bir şekilde kasten veya ihmalen, korumalı bir bilgisayara erişmek, bu tip bir bilgisayara data veya program göndermek,

Bilgisayar şifrelerini veya bilgisayarlara erişmekte kullanılabilecek herhangi bir bilgiyi dağıtmak, başkalarının kullanımına sunmak,

Para veya para hükmünde olan herhangi bir değeri elde etmek maksadıyla, bir bilgisayar veya bilgisayar sistemine zarar verme yönünde tehditler savurmak. (Damon W. D. **Wright,** "Cybercrimes", http://venable.com/internet/cybercrimes.html 10.11.2001 tercüme edip aktaran, Çeken, s. 75).

Ayrıca, daha öncede belirttiğimiz üzere, Amerika Birleşik Devletleri'nde bulunan eyaletlerin hepsi, bilişim suçları ve bazı yetkisiz erişim hallerini suç sayan kanunlar çıkarmıştır. Örneğin, New York' da, suç işlemek veya suça teşebbüs etmek veya herhangi bir ağır suçu daha da ilerletmek niyetiyle yetkisiz giriş yapmanın yanı sıra sadece bilgisayar materyaline izinsiz giriş de bilgisayar suistimali suçu kapsamına girer ve ona göre cezai işlem uygulanır. Washington, başka bir suçun işlenmesini önlemek amacıyla korunan veya bir bilgisayar veya veri tabanın erişiminin hükümet bürosu tarafından muhafaza edildiği bir bilgisayar sistemine veya elektronik veri tabanına kasıtlı ve yetkisiz erişimini içeren, birinci dereceden bilişim suistimali suçuna sahiptir. Alabama Yasası'nda erişim, bilgilendirmek, iletişim kurmak, veri depolamak veya bir bilgisayardan, bilgisayar sisteminden veya bilgisayar ağından veri ele geçirmek olarak tanımlanır. Hawaii'de erişim, bir bilgisayardan, bilgisayar sisteminden veya bilgisayar ağından faydalanmak anlamındadır. (Sandra **Mariana,** http://uir.unisa.ac.za/bitstream/10500/2056/17/03chapter3.pdf)

81 **Yazıcıoğlu**, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 77.

- Ayrıca belirtmek gerekir ki, İtalyan (m.615-ter/3)[82], Fransız (m.323.1/2)[83], Lüksemburg (m.509.1/2)[84] ve Norveç(m.145/3)[85] Ceza Kanunları, bu tür eylemler neticesinde sistemin işleyişinin tamamen veya kısmen bozulmasını veya verilerin yok veya tahrip olmasını verilecek cezalarda artırım sebebi kabul etmektedir. İtalyan CK. "bilgisayar ve sistemlerine girme veya kalma fiilinin" belirli kimseler tarafından görevlerini suistimal ederek veya aşikar bir silahla veya eşya yahut şahıslar üzerinde cebir kullanarak işlenmesini cezayı artıran hal olarak düzenlerken (m.615-ter/1 ve 2), Yunan CK. "hukuka aykırı olarak girme" fiilinin hak sahibinin müstahdemi sıfatıyla çalışanlar tarafından işlenmesi durumunu cezayı artıran hal olarak kabul etmektedir (m.370.C/3)[86].

Mukayeseli hukukla ilgili olarak benzer açıklamalar için bknz. **Mariana**, http://uir.unisa.ac.za/bitstream/10500/2056/17/03chapter3.pdf; Ahmet **Caner Yenidünya/**Olgun **Değirmenci**, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul, Legal Yayınevi, 2003, s. 68; Levent **Kurt**, s. 155; **Pallı**, s. 120, 121; Tunç **Demircan**, Bilişim Alanında Suçlar, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yayınlanmamış Yüksek Lisans Tezi, Konya, 2007, s. 41, 42.

82 İtalyan CK. m.615-ter/3: *"3) Eğer fiil, sisteme zarar verir veya tahrip ederse yahut kısmen veya tamamen işlemesine engel olursa veyahut buralardaki veri, bilgi veya programlara zarar verir veya tahrip ederse; Ceza bir seneden beş seneye kadar ağır hapis cezasıdır*" (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 77).

83 Yeni Fransız CK. m.323.1/2: *"Bu eylem (hukuka aykırı olarak girme veya kalma) sistemdeki verilerin tahribi veya değişmesiyle, sistemin işlevinin bozulmasıyla sonuçlanırsa ceza iki sene hapis ve 200.000 frank para cezasıdır"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 77).

84 Lüksemburg CK. m.509.1/2: "*Bu eylem sistemdeki verilerin tahribi veya değişmesiyle, sistemin işlevinin bozulmasıyla sonuçlanırsa hapis cezası iki aydan iki seneye kadar ve para cezası 50.000 Franktan 500.000 Franka kadardır"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 77).

85 Norveç CK. m.145/3: *"Hukuka aykırı olarak öğrenmek için bilginin elde edilmesi veya kullanılması sonucunda bir zarar oluşursa veya eylem hukuka aykırı bir menfaat temin etmek maksadıyla yapılırsa iki yıla kadar hapis cezası verilir"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 78).

86 **Yazıcıoğlu**, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 78.

Japonya'da da 128 sayılı Kanun'un 3'üncü maddesi gereği, bir kimsenin bilgisayarına yetkisiz erişim yasaktır[87].

İslam hukuku doktrininde de Nur Suresi 27 nci ayetten[88] ve Hucurat Süresi 12'nci ayetten[89] ve ayrıca Hz.Muhammed (SAV) 'in *"Bakmak için bile izin isteyiniz"* hadisiyle *"Kişinin kesin izni olmadan bir müslüman'ın başkasının malını alması yasaktır"* hadisinden yola çıkılarak başkasının bilgisayarında depolanmış kişisel dosyalarına bakmanın yasak olduğu, elektronik ortamda da mahremiyetin korunduğu sonucuna ulaşılmıştır[90].

5237 s. TCK'ya kaynak teşkil etmesi nedeniyle Alman ceza hukukundaki durumu özel olarak değerlendirmek gerekirse;

---

87 Bu maddeye göre aşağıdaki hallerden birisi varsa, bilgisayara yetkisiz erişimden söz edilir:

Erişilmesi (girilmesi) kontrol altında olan (sınırlandırılan) ve kişiye özel şifreyle erişim imkanı olan bilgisayara telekomünikasyon hattı yoluyla girilmesi (sistem yöneticisi, erişim (şifre) kontrolünü yapan yetkili ve diğer yetkililerin fiilleri bunun dışındadır).

Girişi kontrol edebilen özel bir bilgisayardaki işlemle belli kişilerin kullanımına tahsis edilmiş olan bilgisayara, bilgiye (şifreyle girilenler hariç) telekomünikasyon hattı yoluyla girilmesi veya giriş kontrol fonksiyonunu kaldıracak şekilde işlem yapılması (sistem yöneticisi, erişim "şifre" kontrolünü yapan yetkili ve diğer yetkililerin fiilleri bunun dışındadır).

Özel bir bilgisayarda yapılan işlemle sınırlı kişilerin kullanımına tahsisli olan ve başka bir bilgisayarla girişi kontrol edilen bilgisayarların, yetkisiz erişimle telekomünikasyon hattı yoluyla başkaları (kamu) tarafından kullanılabilir hale getirilmesi.

128 sayılı Kanun'un 4. maddesine göre de, hiç kimse diğer bir kimsenin bilgisayara giriş şifresini bunun özel bir bilgisayara giriş şifresi olduğunu belirterek veya bunun giriş şifresi olduğunu bilebilecek bir kişinin talebi üzerine başkalarına veremez (girişi kontrol eden yöneticileri veya o şifreyle girmeye yetkili diğer kişiler hariç olmak üzere).

128 sayılı Kanun'un 9. maddesine göre ise her kim, 4. maddenin hükümlerini ihlal ederse, 300.000 yenden fazla olmamak üzere para cezasına çarptırılır (**Karagülmez,** s. 118).

88 Allah der ki: "*Ey inananlar, kendi evlerinizden başka evlere, izin alıp halkına selam vermeden girmeyin. Herhalde bunun, sizin için daha iyi olduğunu düşünüp anlarsınız"* (**Nur Suresi,** 27).

89 Allah der ki*: "Ey inananlar, zandan çok sakının. Zira zannın bir kısmı günahtır. Birbirinizin gizli şeylerini araştırmayın; biriniz diğerinizi arkasından çekiştirmesin*"(**Hucurat Suresi,** 12).

90 Al-A'ali **Mansoor**, "Cybercrime and the Law: An Islamic View", Webology, Volume 4, Number 3, September, 2007, http://www.webology.ir/2007/v4n3/a46.html 20.07.2010.

Almanya'da 15 Mayıs 1986 tarihli Ekonomik Suçların Önlenmesiyle İlgili Kanun bilişim ceza hukukundaki ilk hükümleri içermekte olup bir başlangıç sayılmaktadır. Bu kanunla elektronik ve bilgisayar destekli yeni saldırı şekillerini önlemek ve oluşabilecek kanun boşluklarını gidermek amacıyla bilişim suçları ceza hükümlerine eklenmiştir ve evrakta sahtecilikle ilgili ceza hükümleri değiştirilerek genişletilmiştir (Al.CK. § 269 ve § 270 maddelerinde yer alan ve delil niteliği taşıyan belgelerde sahtecilik ile bilgi işlem yoluyla hukuki işlemlerde sahtecilik). Böylelikle Al.CK. § 202a'ya göre verilerde casusluk, aynı Kanunun § 303a ve § 303b uyarınca verilerin değiştirilmesi ve bilgisayar sabotajı suç sayılmaktadır. Bu maddelerde özellikle ekonomik ve idari alanlardaki bilgi işlemlerin korunmasının ön planda tutulmasından dolayı, bilgi depolama ve bilgi işlem cihazlarına yönelik dış müdahaleler ve sabotaj eylemleri önlenmek istenmiştir[91].

Alman Ceza Kanunu'nun 202a maddesinde[92], TCK'nın 243'üncü maddesinde bulunduğu üzere, hukuka aykırı olarak bilgisayar ve sistemlerine girme ve kalma başlı başına suç haline getirilmemiş, sistemdeki veriyi elde

---

91 Brian **Valerius**, "Almanya'da İnternet Ceza Hukuku" Alman Türk Karşılaştırmalı Ceza Hukuku, tercüme edip aktaran, Rabia Ünlü, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi Yayınları, Yayın no:17, 2010, s. 356

92 "Alman CK. m.202a/1: "*Her kim yetkisiz olarak kendisi veya bir başkası yararına, kendisine ait olmayan ve başkalarının girişine açık bulunmayan ve emniyet altına alınmış verileri ele geçirirse üç yıla kadar hapis veya para cezasıyla cezalandırılır"* (tercüme edip aktaran, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 78).

Alman Ceza Kanunu'na ilişkin olarak doktrinde *"Alman Ceza Kanunu'nun 202a maddesi, veri ajanlığı suçuna önlem alır ve kişinin üstüne vazife olmayan ve yetkisiz erişimlere karşı özellikle korunan veriyi yetkisiz olarak ele geçiren herhangi bir insanın suçlu olduğunu söyler. Alman Ceza Kanunu elektronik veriye yoğunlaşır. Ayrıca verinin doğrudan görünür olmasının gerekmediğini belirtir. Temin unsurlarının tümü muhtemelen verinin silinmesini veya en azından bir kopyasının yapılmasını gerektirir"* denilmiştir (**Mariana,** http://uir.unisa.ac.za/bitstream/10500/2056/17/03chapter3.pdf).

Gercke'de açıklamalarında *"Kelimelerin değiştiği kanunlarda kelimelere bağlı kalmak gerekmektedir. 202a maddesinden önce eski kanuna göre yetkisiz erişim suç değilken kanun değişikliği nedeniyle mahkemeler bu tür faaliyetleri cezalandıracaktır"* demiştir (Marco **Gercke,** New German Laws on Cybercrime, http://www.securityfocus.com/columnists/448/2).

etmek cezalandırılmıştır[93]. Bu nedenle doktrinde bir görüş[94] bilişim sistemlerine girmeyi suçun oluşumu için yeterli görmeyip verilerin ele geçirilmesi koşulunu da aramakla Alman Ceza Kanununu yetersiz görmektedir. Burada dikkat edilmesi gereken diğer bir nokta ise, yetkisiz girişten söz edebilmek için bilişim sistemine yetkisiz girişe karşı özel olarak korunan bir sistem olması gereğidir. Böylece Alman Ceza Kanunu'nun 202a maddesi ile herhangi bir veri değil, korunmuş veriler güvence altına alınmaktadır[95]. Alman Ceza Kanunu'nun 202c maddesinde[96] ise; hazırlık hareketlerinin cezalandırılacağı düzenlenmiştir[97].

Saf erişim hükümleri, hasar meydana gelsin ya da gelmesin, katı erişim hükümleridir[98]. Ancak yukarıda da belirttiğimiz üzere bazı ülkelerde, bilgisayara yapılan saf yetkisiz erişim, failin amacı ya da verdiği hasarın boyutu ne olursa olsun, suç sayılmaktadır. Buna göre, herhangi bir bilgisayara,

---

93 Benzer açıklama için bknz. **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi", s. 78.

94 **Mariana,** http://uir.unisa.ac.za/bitstream/10500/2056/17/03chapter3.pdf; **Yazıcıoğlu**, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 78; Önder, s. 505.

95 Benzer açıklamalar için bknz. Eric **Hilgendorf**, "Yeni Bilgisayar Ceza Hukuku", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt:V Sayı:2 yıl 2008, s. 129, tercüme edip aktaran Aylin **Dağlar**; **Karagülmez**, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, s. 332.

96 "Veri Casusluğunun ve Verileri İletirken Ele Geçirilmesinin Hazırlığı" başlıklı Alman CK. m.202c: (1) Her kim 202a veya 202b maddelerinde belirtilen suçların işlenmesini hazırlamak üzere,

1. verilere giriş yapmayı sağlayan (202a veya 202b) şifre vesair güvenlik kodlarını veya,
2. Bu tür fiilleri işlemeyi amaçlayan bilgisayar programları

Üretir, kendisine veya bir başkasına sağlar, satar, bir başkasına verir, yarar veya sair bir şekilde ulaşılabilmesini sağlarsa, bir yıla kadar hapis cezası veya adli para cezasıyla cezalandırılır.

(2) 149'uncu maddenin 2 ve 3'üncü fıkraları kıyasen uygulanır

Gercke açıklamalarında *"AKSSS'nin 6'ncı maddesinden farklı olarak 202c maddesi suçlamayı öncelikli olarak belli suçları işlemek için tasarlanan gereçlerle sınırlandırmamaktadır"* demiştir **Gercke,** http://www.securityfocus.com/columnists/ 448/2

97 Alman Ceza Kanunu için bknz. **Brian Valerius**, "Almanya'da İnternet Ceza Hukuku" Alman Türk Karşılaştırmalı Ceza Hukuku, Çeviren Rabia **Ünlü**, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi Yayınları, Yayın no:17, 2010, s. 359.

98 **Schjolberg/Hubbard,** s. 11.

bilgisayar sistemine, bilgisayar ağına, bilgisayar yazılımına, bilgisayar programına ya da bu tip bir bilgisayarın, bilgisayar sisteminin, bilgisayar programının ya da bilgisayar ağının içinde bulunan veriye yapılacak istemli ya da istemsiz yapılacak her yetkisiz erişim suç sayılmaktadır. Örneğin; Malezya Bilişim Suçları Yasası, güvenlik önlemlerinin ihlal edilip edilmediğine bakılmadan bilgisayarlara yapılan yetkisiz erişimi cezalandırılmaktadır[99].

TCK'nın 243'üncü maddesinde düzenlenen suçun neticesine gelince; kanaatimizce kanun metninde yer alan sisteme girme ve kalma bir hareket değil neticedir. Yani, yukarıda belirttiğimiz üzere, herhangi bir şekilde (serbest hareketli eylemle) sisteme girilmesi ve kalınması halinde netice gerçekleşmiş olur. Kanun metninde ayrıca bir netice aranmamıştır. Burada önemli olan failin sisteme girdikten sonra suçu oluşturmaya yetecek kadar süreyle sistemde kalmasıdır. Bu nedenle suçun varlığı için harekete değil, neticeye bakılmalıdır. Failin hareketleri sırasında, suça konu sistemden bir şey öğrenmiş olması veya mağdurun bir zarara uğramış olması şart değildir. Ancak, hareket sürecinde fail, sistemin içerdiği verilerin yok olmasına veya değişmesine neden olmuşsa (koşulları da varsa) 243 (3) maddesindeki suçun nitelikli halinden hüküm verilebilir. Maddenin gerekçesinde de "sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur" denilerek bu durum vurgulanmıştır.

3.1.2. Fail

Her suçun mutlaka bir faili vardır ve fail sadece insandır. Suç failinin insan olması kuralının istisnası yoktur[100]. 5237 s. TCK'nın 20'nci maddesinde de cezaların kişiselliği ilkesi benimsenmiştir. Bu nedenle tüzel kişiler suçun faili olamazlar[101]. Nitekim TCK'nın 20'nci maddesinin gerekçesinde *"Sadece gerçek kişiler suçun faili olabilir ve sadece gerçek kişiler hakkında ceza yaptırımına hükmedilebilir"* denilerek; kim hakkında ceza müeyyidesine hükmedilebiliyorsa, ancak o kimsenin fail olabileceğine işaret edilmiş

---

99 **Kadir**, s. 627.

100 Zeki **Hafızoğulları**/Muharrem **Özen**, Türk Ceza Hukuku Genel Hükümler, Ankara, U-S-A Yayıncılık, 2008, s. 393.

101 Tüzel kişiler hakkında benzer açıklamalar için bknz. Sacit **Yılmaz,** "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", Türkiye barolar Birliği Dergisi, 2011 (92), s. 87; **Soyaslan,** s. 609.

olunmaktadır[102]. Ancak tüzel kişiler hakkında güvenlik tedbirlerine hükmolunabilir.

Bu açıklamalar ışığında inceleme konumuza döndüğümüzde, 243'üncü madde metninde cezalandırılacak şahıs olarak "kimse" tabiri kullanılıp herhangi bir özellik aranmadığından bu suçun faili herkes olabilir. Bu kabul karşısında bilişim sistemine hukuka aykırı olarak giren veya orada kalmaya devam eden herkes bu suçun failidir[103].

Bu suçun failleri genellikle bilişim korsanı, hacker ya da craker olarak adlandırılmaktadır.

Bilişim suçları ilk zamanlarda beyaz yaka suçlarının (white-collar crime)[104] bir çeşidi olarak değerlendirilmekteydi[105]. Çünkü henüz bilişim sistemlerinin gelişmediği ve yaygınlaşmadığı bir dünya da, bu suçlar ancak bilgisayarın mevcut olduğu ortamlarda, bilgisayarla irtibatlı bir işte çalışan kimseler tarafından işlenebilmekteydi. Diğer bir değişle suç faillerinin mesleki faaliyetleri ile işledikleri suçlar arasında önemli bir bağlantı bulunmaktaydı. Ancak günümüzde bilişim sistemlerinin gelişmesi, hayatın her alanına yayılması, evlerde, iş yerlerinde, okullarda, üniversitelerde ve hatta umuma açık mahallerde bile bir bilişim sistemine ulaşmanın ve ondan faydalanmanın kolaylığı, öncelikle bilişim alanındaki suç faillerinin teknolojik bilgiye sahip sınırlı sayıda kimseler olarak belirlenmesini imkansız hale getir-

---

102 **Hafızoğulları/Özen**, s. 395, 396. Benzer açıklamalar için bknz. **Artuk/Gökçen/Yenidünya,** Ceza Hukuku Özel Hükümler, s. 21; **Dülger**, s. 216.

103 Benzer açıklamalar için bknz. **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4637; **Doğan,** s. 294; **Yaşar/Gökçan/Artuç**, s. 6738; **Malkoç**, s. 1667; **Yazıcıoğlu**, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 82; Nurullah **Aydın**, s. 382; **Esen** s. 628; **Dülger**, Bilişim Suçları, s. 214; **Taşkın**, Bilişim Suçları, s. 23.

104 Beyaz yaka suçu (white-collar crime), bir kimsenin sahip bulunduğu mesleğinden kaynaklanan sosyal statüsünü ve kendisine duyulan güveni kötüye kullanarak işlediği suç teşkil eden eylemleri ifade etmektedir. **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4637.

105 Emin Doğan **Aydın**, Bilişim Suçları ve Hukukuna Giriş, Ankara, Doruk Yayınları, 1992, s. 30; Yüksel **Ersoy**, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", Prof.Dr Yılmaz GÜNAL'a Armağan, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, Cilt:49, No:3-4, 1994, s. 167.

miştir[106]. Ancak belirtmek gerekir ki, bu tür suçların işlenebilmesi için, belli bir düzeyde bilgi donanımına sahip bulunmak gerekse de, bu husus sadece şahsın bu suçu gerçekleştirebilmesi için gerekli olup kanunen aranan bir özellik değildir[107].

Son olarak belirtmeliyiz ki, suçta failin belirlenebilmesi için, fiilin bilişim sisteminin hangi unsuruna yöneldiğinin tespit edilmesi gerekmektedir. Fiil eğer bilişim sisteminin kendisine yöneltilmişse sistemin kendisi üzerinde, verilere yöneltilmişse veriler üzerinde, hem bilişim sistemine hem de verilere yöneltilmişse her ikisinin de üzerinde kullanım; mülkiyet ve tasarruf yetkisinin kimde olduğunun ortaya konması gerekecektir[108]. Zira mülkiyet sahibinin kiracısının ya da kiracının mülkiyet sahibinin yetki alanına müdahalesi gibi durumlar söz konusu olabilecektir.

3.1.3. Mağdur

Mağdur, suç tanımıyla korunan hak ve menfaatin sahibi olan kişidir; yani, suçtan doğrudan doğruya etkilenen[109] kişidir. Bu kişi, suçun olumsuz etkilerini doğrudan doğruya üzerinde hisseder. Suç tanımıyla korunan hak ve menfaatin dışında kalan hak ve menfaatlerin ihlal edildiği hallerde, bu hak ve menfaatin sahipleri ise dolaylı olarak suçtan zarar görenler olarak adlandırılır. Şikayetçi ise TCK'nın 73'üncü maddesi uyarınca takibi şikayete bağlı suçlarda suçtan zarar gören kişidir[110].

---

106 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4637.

107 **Kurt,** s. 241.

108 **Dülger,** Bilişim Suçları, s. 232; **Taşkın,** Bilişim Suçları, s. 43.

109 Mağduru *"suçtan doğrudan zarar gören kişi"* olarak tanımlayan Kunter/Yenisey/Nuhoğlu suçtan zarar göreni de *"işlenen suçtan zarar gören mağdur dışındaki kişiler"* olarak tanımlamaktadır (Nurullah **Kunter/**Feridun **Yenisey/**Ayşe **Nuhoğlu,** Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 17.Baskı, İstanbul, Beta Yayınevi, 2009, s. 341).

110 Nur **Centel/**Hamide **Zafer**, Ceza Muhakemesi Hukuku, 5.Baskı, İstanbul, Beta Yayınevi, 2008, s. 806, 807.

Ancak Kunter/Yenisey/Nuhoğlu şikayetçi kelimesini dar anlamda anlayıp sadece soruşturulması ve kovuşturulması şikayete bağlı olan suçlarla sınırlı tutmanın CMK'nın 234'üncü maddesinde tanımlanan birçok hakkı şikayetçiden alma sonucunu doğuracağından eleştirmektedir (**Kunter/Yenisey/Nuhoğlu**, s. 341).

Doktrinde tüzel kişilerin mağdur olamayacağı, yalnızca suçtan zarar gören olabileceği yönünde görüşler[111] bulunmakla birlikte kanaatimizce tüzel kişilerde suçun mağduru olabilir[112]. Zira biz mağduru suç tanımıyla korunan hak ve menfaatin sahibi olan kişi olarak kabul edip inceleme konusu suçta da korunan temel hukuki menfaatin sistemin güvenilirliği olduğunu kabul ettiğimizde, sistem sahibi pek çok zaman tüzel kişi olacağından, onu mağdur kabul etmemiz gerekecektir. Bu durumda bir bankanın bilişim sistemine girerek, müşteri bilgilerinin incelenmesi durumunda, bilgileri incelenen her bir müşteri suçun mağduru olduğu gibi, banka tüzel kişiliği de mağdurdur. Zira sisteme yetkisiz girişle toplumun o bankaya güveni kalmayacağından ciddi şekilde ve doğrudan failin eyleminden etkilenmiş olmaktadır[113].

Bu suçta mağdur, bilişim sistemine hukuka aykırı olarak girilmesinden ve orada kalınmasından dolayı hakları tehlikeye giren kişidir. Failin eylemi ile birden fazla kimsenin hakkı ihlal edilmekte ise, bu kimselerin hepsi anılan suçun mağdurudur[114]. Örneğin; bir kimsenin kişisel dosyasını arkadaşının bilgisayarında muhafaza ettiği düşünülürse, bu bilgisayara girilerek söz

---

111 Örneğin bknz. Mehmet Emin **Artuk/**Ahmet **Gökçen/**Ahmet Caner **Yenidünya,** Ceza Hukuku Genel Hükümler, 3 Basım, Ankara, Turhan Kitapevi, 2007, s. 307; **Koca** Mahmut/**Üzülmez** İlhan, Türk Ceza Hukuku Genel Hükümler, Ankara, Seçkin Yayınevi, 2008, s. 133; **Sacit** Yılmaz, "5237 Sayılı TCK'nın 244.Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", s. 87.

112 Mağduru en kolay tanımının suçtan zarar gören kişi olduğunu belirten Ünver ve Hakeri suçtan zarar görenin de gerçek ve tüzel kişi olabileceğini belirterek, tüzel kişilerinde mağdur olabileceğini kabul etmiş olmaktadır (Yener **Ünver/**Hakan **Hakeri,** Ceza Muhakemesi Hukuku, 3.Baskı, Ankara, Adalet yayınevi, 2010, s. 304).

Nitekim inceleme konumuz sanal alandaki girişin fiziki ortamda gerçekleşen haline örnek olarak gösterilebilecek TCK'nın 154'üncü maddesindeki "Hakkı Olmayan Yerlere Tecavüz" suçunu açıklarken Özbek/Kanbur/Doğan/Bacaksız/Tepe'de mağdurun gerçek kişi olabileceği gibi, kamu ya da özel hukuk tüzel kişisinin de olabileceğini belirtmiştir (**Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 667).

Bu suçta tüzel kişilerinde mağdur olabileceği konusunda ayrıca bknz. **Doğan**, s. 295; **Soyaslan**, s. 605; **Yenidünya**, s. 1027

113 Benzer görüş için bknz. **Doğan**, s. 295. Aksi görüş için bknz. **Artuk/Gökçen/ Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4639, 4640; **Yaşar/Gökçan/Artuç,** s. 6739.

114 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4639, 4640; **Doğan**, s. 295; **Dülger,** Bilişim Suçları, s. 217; **Taşkın**, Bilişim Suçları, s. 24; **Kurt,** s. 242; **Yaşar/ Gökçan/Artuç,** s. 6739.

konusu dosyaya ulaşılması halinde de hem bilgisayarın sahibinin hem de veri sahibinin mağdur olduğu şüphesizdir[115].

Burada dikkat edilirse hak sahibi olma tabirini kullanmış bulunmaktayız. Bilişim sisteminin üzerinde hak sahibi olmak, ya mülkiyet hakkı sahibi olmakla, ya da başka bir kısım sözleşmelerle (kira, ariyet, finansal kiralama gibi) elinde bulundurmakla söz konusu olabilir. Örneğin; finansal kiralama yoluyla almış olduğu bilgisayarları ticari bir üretimde kullanan kiracının bilgisayarlar üzerinde mülkiyet hakkı bulunmamakta, finansal kiralama şirketi sistemlerin sahibi bulunmaktadır. Bu konumda olan kiracının bu sistemler üzerinde bulunan zilyetlik hakkı gereğince suçun mağduru olduğu kabul edilecektir. Bu örnekte, finansal kiralama şirketi, sistemler üzerinde mülkiyet hakkı bulunsa da, bu suç temelde mülkiyet hakkını korumadığından, suçun mağduru olarak kabul edilemeyecektir. Çünkü verilerin gizliliği ve özel alanın masuniyeti ihlal edilen bilişim sistemi üzerinde zilyetliğini sürdüren finansal kiralayandır[116]. Kanaatimizce sistemin güvenilirliği korunan bir değer olduğundan kiralayan şirket olay nedeniyle yeni kiracı bulmakta zorlanacağından o da suçtan zarar gören değil mağdurdur. Bu noktada belirtmeliyiz kiralayan kiracının sistemine zarar verirse, sistemin maliki olmasına rağmen fail de olabilecektir. Zira daha önceden belirttiğimiz üzere asıl korunan mülkiyet hakkı değildir.

3.1.4. Suçun Konusu

Üzerinde suçun meydana geldiği, yasada belirtilen hareketin yönelik olduğu eşya veya şahsın fiziki, maddi yapısı, bünyesi suçun konusunu oluşturmaktadır. Suçun konusu ile korunan hukuki değer arasındaki farka da işaret etmek gerekirse; suçun konusu kısaca hareketin yönelik olduğu ve ceza normunda belirtilen kişi ya da şey iken, korunan hukuki değer suç tipinin ihdas edilmesiyle korunmak istenen değerdir[117].

TCK'nın 243'üncü maddesinin birinci fıkrasında düzenlenen suçun konusu hukuka aykırı olarak içine girilen ve orada kalmaya devam edilen

---

115 **Artuk/Gökçen/Yenidünya,** Türk Ceza Kanunu Şerhi, s. 4639, 4640.

116 **Kurt,** s. 163.

117 Benzer yönde açıklamalar için bknz. **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4639, 4640; T**aşkın,** Bilişim Suçları, s. 24; **Dülger,** Bilişim suçları, s. 217; **Kurt,** s. 162.

bilişim sisteminin soyut varlığı iken, ikinci fıkrada düzenlenen indirim sebebinin konusu bedeli karşılığında yararlanılan bilişim sistemi olup, üçüncü fıkrada düzenlenen suçun konusunu ise bilişim sisteminin içerdiği veriler oluşturmaktadır[118].

Bu suçun konusu, bilişim sisteminin bütünü de bir kısmı da olabilir[119]. Ayrıca belirtmek gerekirse, gerçek bir kişinin evinde kullandığı kişisel bilgisayarına ait bilişim sistemi de bir kamu kurumunda kullanılan bilişim sistemi de bu suçun konusunu oluşturabilecektir.

3.1.5. Suça Etki Eden Sebepler

Suçu etkileyen haller olan daha az ya da fazla cezayı gerektiren haller, suçun varlığı için bulunmaları zorunlu olan kurucu unsurlara eklenen sebeplerdir. Suçun daha ağır veya daha hafif sayılmasını ve bunun sonucu olarak da cezanın artırılıp indirilmesini gerektirirler. Ancak, bulunmamaları halinde suçun varlığına zarar vermezler. Bulundukları zamanda suçun hukuki niteliğinin değişmesine yol açmazlar[120].

3.1.5.1. *Daha Az Cezayı Gerektiren Haller*

TCK'nın 243 (2)'nci maddesinde yetkisiz giriş suçunun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hali daha az cezayı gerektiren hal olarak düzenlenmiştir. Bu fıkranın uygulanabilmesi için ortada bir bilişim sistemi olması ve bu bilişim sisteminin de bedeli karşılığı yararlanılan bir sistem olması gerekir. Diğer bir değişle, failin bedelini ödeyerek hukuka uygun olarak girebileceği bir sisteme, bedeli ödemeksizin girmesi ve orada kalmaya devam etmesi durumunda bu fıkra hükümleri uygulanır[121].

---

118 Benzer açıklamalar için bknz. Mahmut **Koca**, "Hukukumuzda TCK'nın 244 ncü maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı, Ankara, Yargıtay Başkanlığı Yayını, 2009, s. 92; **Yaşar/Gökçan/Artuç**, s. 6739; **Eker,** s. 124, 125; **Yılmaz**, "5237 Sayılı TCK'nın 244.Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", s. 88; **Soyaslan,** s. 609; **Yenidünya,** s. 1027.

119 **Kurt,** s. 150.

120 Nur **Centel**/Hamide **Zafer**/Özlem **Çakmut,** Türk Ceza Hukukuna Giriş, İstanbul, BetaYayınevi, 2005, s. 593.

121 **Yaşar/Gökçan/Artuç,** s. 6750.

Bu noktada kanaatimizce bedelin ne olduğu, bedeli karşılığında yararlanılan sistemlerin hangileri olduğu, decoder ve otomatlar ile internet kafeler ve benzeri yerlerin bu kapsamda olup olmadığı, bu indirim sebebinin yerinde olup olmadığı, madde metninde geçen "Yukarıdaki fıkrada tanımlanan fiillerin" denilmek suretiyle çoğul ifadenin ne anlama geldiği hususlarının tartışılması gerekmektedir.

Bedel, Türk Dil Kurumu Büyük Sözlüğünde, *"1.Değer, fiyat, kıymet 2. Bir şeyin yerini tutabilen karşılık"* şeklinde tanımlanmıştır[122].

Fıkradaki "bedeli karşılığında yararlanılabilen" ibaresindeki "bedel"i yalnızca para olarak anlamamak gerekir. Çünkü buradaki bedel, karşılık anlamındadır. Bir hizmetin karşılığı genellikle para ile ödenirse de kimi zaman başka şey de bedel kavramına girebilir. Örneğin internet ortamında abonelerine hizmet sunan bir site, kendisine makale gönderilmesini ya da sitesine en az beş kişinin abone edilmesinin sağlanmasını bedel olarak kabul etmişse, bu siteye yönelik madde kapsamındaki suçta da (2) numaralı fıkranın koşulları gerçekleştiğinden cezada indirime gidilmelidir[123].

"Bedeli karşılığı yararlanılabilen sistem" kavramı bilişim suçları bakımından Türk Ceza Kanununa ilk defa girmiş[124] olmasına rağmen, bu kavram hakkında kanunun 243'üncü maddesinde ya da gerekçesinde bir açıklama yapılmamıştır[125].

Bedeli karşılığı yararlanılabilen sistem kavramına, web sitelerinin girdiğinde tereddüt yoktur. Bunlara örneğin; internet ortamındaki ücreti karşılığında abonelerinin kullanımına açık elektronik arşiv merkezleri, elektronik gazeteler, elektronik kütüphaneler ya da tümüyle şifreli kullanıma açık benzer nitelikteki web siteleri gösterilebilir. Bu sistemlere, herkesin girmesi mümkün değildir. Ancak, belli süreler için öngörülen bedel ödendiği takdirde, genellikle müşteriye verilen şifre ile bu sistemlere girilebilmektedir. Aynı şekilde, bir kuruluş tarafından belli bir sistemin (örneğin anlaşmayla cep telefonlarına bilişim sistemi üzerinden reklam için mesaj yollanması gibi) bedel karşılığı sunulması da bu kapsamda değerlendirilebilir[126].

---

122 http://tdkterim.gov.tr/bts/ 05.03.2011.

123 **Karagülmez,** s. 174.

124 Benzer açıklamalar için bknz. **Karagülmez,** s. 173.

125 **Yenidünya**, s. 768.

126 **Karagülmez,** s. 173, 174. Benzer açıklamalar için bknz. **Dülger,** Bilişim Suçları, s. 71, 72.

TCK'nın 163 (1) maddesinde açıkça otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan yararlanan kişinin cezalandırılacağı belirtildiğinden, otomatlar TCK'nın 243 ve 244'üncü maddeleri kapsamında değerlendirilemezler[127].

Bu nitelikli unsur bakımından dekoderler üzerinde de durmak gerekirse; dekoderler, kendilerine gönderilen şifreli bilgiyi alarak işleme tabi tutup üzerindeki yüklü programları veri üzerine uygulayıp bundan farklı bir veri çıkartıp alıcıya ulaştırdığından kanımızca bilişim sistemi olarak değerlendirilebilir. Ancak kanun koyucu "karşılıksız yararlanma" başlığı taşıyan TCK'nın 163 (2)'nci maddesinde; "telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan" kimsenin cezalandırılacağını belirtmiştir. Bu itibarla yasadaki özel düzenleme dolayısıyla dekoder, Türk ceza hukuku bakımından TCK'nın 243'üncü maddesi kapsamında bir bilişim sistemi değil, 163 (2)'nci maddesi kapsamında bir aygıt olarak değerlendirilmelidir[128].

İnternet kafe ve internet bağlantı servisini sağlayan sistemlerin durumuna gelince; bu konuda da doktrinde farklı görüşler bulunmaktadır. Birinci

---

127 163'ncü maddenin gerekçesinde *"Madde metninde karşılıksız yararlanma suçu tanımlanmıştır. Otomatlar aracılığıyla sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan yararlanmak, karşılıksız yararlanma suçunu oluşturmaktadır. Otomatlar aracılığıyla satışa sunulan hizmetlerden, otomatın teknik işleyişini devre dışı bırakan müdahalelerle, bedeli ödemeksizin yararlanılması durumunda, ortada bir taşınabiliri mal bulunmadığı için, hırsızlık suçu oluşmayacaktır. Örneğin toplu taşıma sistemlerinde yolcuların geçişlerini kontrol eden otomatlara müdahale edilmek suretiyle ücret ödemeksizin yolculuk yapılması durumunda, karşılıksız yararlanma suçunun oluştuğunu kabul etmek gerekir. Burada, bir hilenin varlığından söz edilemez. Çünkü burada herhangi bir kişi aldatılmamaktadır. Yapılan müdahale ile bir otomatın teknik işleyişinin devre dışı bırakılması durumunda, bir hilenin varlığından söz edilemez. Çünkü dolandırıcılık suçu açısından hilenin varlığı için muhatabın mutlaka insan olması gerekir"* denilmiştir (Gerekçe için bknz. **İzzet Özgenç**, Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), Ankara Açık Ceza İnfaz Kurumu Matbaası, 3.Basım, 2006, s. 877).

Benzer açıklamalar için bknz. **Dalkılıç,** s. 221; **Yenidünya,** s. 773.

128 **Artuk/Gökçen/Yenidünya,** s. 4651. Benzer yönde açıklamalar için bknz. **Yaşar/Gökçan/Artuç,** s. 6750.

görüş taraftarlarına göre[129], bedeli karşılığı yararlanılan sistem tabirinin içine, internet üzerinden ücret karşılığı hizmet veren web sitelerini, internet kafelerde olduğu gibi bir ücret karşılığı kiralanmış sistemleri, bir kuruluş tarafından bir hizmetin sunulduğu bilişim sistemini, bedel karşılığı internet bağlantı servisinin sağlandığı sistemleri dahil etmek mümkündür. Bizimde katıldığımız ikinci grupta yer alan yazarlar ise[130]; burada kastedilenin bilişim sisteminin kullanıldığı mekanın değil, bizzat bu sistem içerindeki elektronik yapıda sunulan ücretli hizmetlerin olduğunu, bu nedenle, internet kafedeki bilgisayarın ücretsiz kullanılmasının ya da belli süreli internet bağlantı servisinin sağlanmasının bu fıkra kapsamında olmadığını belirtirler. Bizimde katıldığımız bu ikinci görüş gereği internet kafe ve internet bağlantı servisini sağlayan sistemlerin bedelsiz kullanılması halinde diğer koşulları da gerçekleşmişse, TCK'nın 163 (2)'nci maddesi uygulanabilir[131]. Zira, bedelsiz ve izinsiz olarak internet kafede bilgisayar kullanmak ya da internet bağlantı servisini kullanmak bir telefon kulübesinin aldatılarak bedava kullanılmasından farklı değildir.

Böyle bir indirim sebebinin yerinde olup olmadığı konusunda da doktrinde fikir ayrılıkları vardır. İndirimi yerinde gören görüş; kanun koyucunun bu şekilde bir düzenleme yapma nedeninin, bu sistemlerin güvenliğinin korunmasını daha az değerli görmesi olduğunu zira, sistemin sahibinin zaten belli bir bedel karşılığında kullanımı herkese açtığını, korunması gereken sistemin o kadar da değerli olmadığını, herhangi bir mahremiyete sahip olmayan bu sistemlerde çok önemli verilerin, ekonomik hakların veya manevi değerleri ilgilendiren bilgilerin bulunmadığını, failin amacının sadece bedeli dolanmak olduğunu, bu nedenle tehlike suçu olan bu suçta tehlike halinin burada daha az olduğunu[132]; ticari bir gaye ile üçüncü kişilere sunulan verilerin masuniyeti ile faile hiçbir şekilde kullanım veya erişim izni verilmemiş bulunan verilerin masuniyeti arasında fark bulunduğunu, erişim

---

129 **Yaşar/Gökçan/Artuç,** s. 6750. Benzer görüşler için bknz. **Dülger,** Bilişim Suçları, s. 226, 227.

130 **Karagülmez,** s. 174. Benzer açıklamalar için bknz. **Dalkılıç**, s. 221; **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4651; **Doğan**, s. 298.

131 Benzer açıklamalar için bknz. **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4651; **Parlar,** s. 19; **Yenidünya,** s. 1040.

132 **Yenidünya,** s. 1040; **Pallı,** s. 154.

bedelinin özel hukuk kuralları çerçevesinde alma imkanının bulunduğunu, bu nedenle cezanın daha az olmasının birinci fıkrada korunmak istenen hukuki yararla karşılaştırıldığında yerinde olduğunu [133]; suç ile korunan hukuki yararın birinci fıkrada bilişim sisteminin güvenliği ve özel hayatın gizliliği iken, ikinci fıkrada bu yararın, biraz malvarlığının korunmasına doğru kaydığını[134] belirtmektedir. Buna karşılık diğer görüş; böyle bir cezayı azaltan hale neden gereksinim duyulduğunun, yasa koyucunun neyi amaçladığının gerekçede de bulunmadığını, hukuka aykırı olarak girilen sistem eğer bedeli karşılığı yararlanılan bir sistemse, burada fail hakkında hafifletici değil, tam tersine, ağırlaştırıcı neden uygulanması gerektiğini; Zira failin bilişim sistemine hukuka aykırı olarak girmekle zaten öncelikle bilişim sisteminin güvenliğini ihlal ettiğini, ayrıca bununla da yetinmeyerek sistemin gerçek kullanıcısının (malik veya kullanıcı) mali veya manevi haklarına da (kişisel bilgilerin gizliliği gibi) zarar verdiğini[135] belirterek indirimin yerinde olmadığını, tam tersine bu durumun artırım sebebi olması gerektiğini ifade ederler.

Biz, bu suçla korunan hukuki değerler arasında sistem sahibinin menfaatlerinin de güvence altına alındığını kabul ettiğimizden, bedeli karşılığı girilebilen sitelere bedelsiz giriş yapılmasını ayrıca indirim sebebi yapmanın doğru olmadığını düşünmekteyiz. Ayrıca belirtmeliyiz ki, kanaatimizce, bedel karşılığı olup olmadığına bakılmayıp, sadece kamu kurumları bilişim sistemlerine yapılacak girişlerin cezası ile özel hukuk tüzel kişileriyle gerçek kişilerin bilişim sistemlerine yapılacak girişlerde cezada farklılaşmaya gidilmeliydi[136].

"Yukarıdaki fıkrada tanımlanan fiillerin" denilmek suretiyle çoğul ifade ne anlama gelmektedir? 5237 s. TCK'nın 244 (2) maddesindeki "yukarıdaki fıkrada tanımlanan fiiller" ibaresinin, maddenin birinci fıkrasında "girme ve orada kalmaya devam etme" şeklindeki tek bir fiil bulunması karşısında, yerinde bir niteleme olmadığı, buna rağmen "fillerden" söz edilmesinin

---

133 **Yazıcıoğlu**, "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 85.

134 **Yaşar/Gökçan/Artuç,** s. 6749. Benzer açıklamalar için bknz. **Artuk/Gökçen/ Yenidünya,** Türk Ceza Kanunu Şerhi, s. 4650.

135 **Taşkın,** Bilişim Suçları, s. 36, 37; **Dülger,** Bilişim Suçları, s. 227.

136 Benzer açıklamalar için bknz. **Ketizmen,** s. 110.

maddede tereddütlere neden olabilecek bir çelişki olduğu, üstelik maddenin 3'üncü fıkrasında yerinde olarak "bu fiil nedeniyle" ibaresinin kullanıldığı, bu çelişkinin de 244'üncü maddenin 1'inci fıkrasında TBMM Genel Kurulu'ndaki görüşmeler sırasında yapılan, "giren veya orada kalmaya devam eden" ibaresindeki "veya" sözcüğünün "ve" şeklinde değiştirilmesinden kaynaklandığı düşünülmektedir[137].

3.1.5.2. *Daha Fazla Cezayı Gerektiren Haller*

TCK'nın 243(3) maddesinde düzenlenen girme ve kalma nedeniyle sistemin içerdiği veriler yok olur veya değişirse cezanın altı aydan iki yıla kadar hapis cezası olacağı belirtilmiştir. Bu noktada anılan düzenlemenin ayrı bir suç mu, yoksa birinci fıkradaki suçun neticesi sebebiyle ağırlaşmış[138] hali mi olduğu doktrinde tartışmalıdır.

Birinci görüş[139]; TCK'nın 243'üncü maddesinde düzenlenen bilişim sistemine girme suçu kapsamında iki ayrı suçun yer aldığını, bunlardan birincisinin TCK 243 (1)'de düzenlenen ve maddeye adını veren bilişim sistemine girme ve orada kalma suçu olduğunu, diğerinin ise TCK 243 (3)'de düzenlenen bilişim sistemindeki verilerin yok edilmesi veya değiştirilmesi suçu olduğunu, TCK 243 (3)'de bağımsız bir yaptırımın gösterilmesinin de bunu kanıtladığını belirtmektedir.

---

137 Benzer açıklamalar için bknz. Esra **Yaycı**, "Bilişim Suçları" Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı,Ceza ve Usul Hukuku Bilim Dalı, yayınlanmamış yüksek lisans tezi, Ankara, 2007, s. 82; **Karagülmez,** s. 173.

138 TCK'nın 23 ncü maddesi gereği failin kast etmiş olduğu neticeden daha ağır ve başka bir neticeden dolayı sorumlu tutulabilmesi için gerçekleşen netice bakımından en azından taksirle hareket etmiş olması gerekir. Neticesi sebebiyle ağırlaşan suçlarda, ağır neticenin faile yüklenebilmesi için failin suçun temel şekli için kasten hareket etmiş olması, ancak kastettiği suç ve neticeden daha ağır bir neticenin meydana gelmesi gerekir. Neticesi sebebiyle ağırlaşmış suç hakkında ayrıntılı bilgi için bknz. **Artuk/ Gökçen/Yenidünya**, Ceza Hukuku Genel Hükümler, s. 519 vd.

139 Örneğin; bknz. **Malkoç**, s. 1671, **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 85; **Yaşar/Gökçan/Artuç**, s. 6747; **Eker,** s. 124.

Diğer görüş[140] ise; TCK'nın 243 (3) maddesinin ayrı bir suç olarak kabul edilmesinin mümkün olmadığını, burada bilişim sistemine girme ve orada kalmaya devam etme suçunun cezayı artıran bir halinin söz konusu olduğunu, üçüncü fıkrada kanunilik, maddi, manevi ve hukuka aykırılık unsurları olan müstakil bir suç düzenlenmediğini, üçüncü fıkrada suç olarak kabul edilen fiil yani maddi unsurun tarif edilmediğini, "bu fiil nedeniyle" ifadesiyle birinci fıkrada tanımlanan fiile atıf yapıldığını, üçüncü fıkrada tanımlanan suçun ilk fıkrada tanımlanan suçun neticesi sebebiyle ağırlaştırılmış bir hali olduğunu, nitekim madde gerekçesinde de bu hususun açık bir biçimde ifade edildiğini belirtirler.

Kanaatimizce, üçüncü fıkrada cezada artırım miktarı belirtmek yerine doğrudan ceza tayin edilmesi nedeniyle akla bağımsız bir suç olduğu gelebilir ise de; fıkranın başında açıkça birinci fıkraya atıf yapılması, bağımsız suç için gerekli maddi unsurlara yer verilmemiş olunması nedeniyle birinci fıkranın neticesi sebebiyle ağırlaşmış hali olduğunun kabulü gerekir. Bu kabulümüz nedeniyle bilişim sistemine yasadışı giriş sağlayıp orada kalan failin bilişim sistemindeki verilerin bozulması ya da değişmesinden dolayı sorumlu tutulabilmesi için TCK'nın 23'üncü maddesi gereğince en azından taksirle bu değişim veya zarara sebebiyet vermesi gerekecektir. Kaldı ki, bu fıkrayı bağımsız bir suç kabul edersek bu maddenin uygulanması mümkün olamayacaktır. Zira verilere kasıtlı müdahale TCK'nın 244 (2) maddesinde açıkça düzenlenmiş olup fikri içtima bakımından cezası da daha ağırdır. Verilere taksirli müdahaleden dolayı da uygulanamaz. Çünkü bir taksirli eylemden dolayı ceza verebilmek için kanun metninde taksirli eylemin cezalandırılacağının açıkça düzenlenmesi (ya da eylemin başka bir suçun neticesi sebebiyle ağırlaşmış hali olması) gerekir. TCK'nın 244 (3) maddesinde ise taksire ilişkin bir cümle bulunmamaktadır. Diğer bir değişle, buradaki düzenlemenin neticesi sebebiyle ağırlaşmış hal olarak kabulümüz sayesinde

---

[140] Benzer açıklamalar için bknz. İlker **Tepe**, "İnternet (Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukuku'ndaki Yeni Gelişmeler" Alman Türk Karşılaştırmalı Ceza Hukuku, Yayına Hazırlayanlar Prof Dr Dr. Eric HİLGENDORF, Prof Dr Yener ÜNVER, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi Yayın No:17, 2010, s. 281; **Kurt,** s. 152; **Doğan,** s. 298; **Artuk/Gökçen/Yenidünya** s. 4634; **Özbek/Kanbur/Doğan/Bacaksız/Tepe,** s. 903; **Değirmenci,** "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", s. 204; **Soyaslan**, s. 613; **Parlar,** s. 19; **Yenidünya,** s. 1041.

sistemin içerdiği verilerin, failin taksirli hareketiyle zarara uğraması durumu cezalandırılabilir hale gelmektedir. İlliyet bağının olmadığı veya kesildiği ya da verilerin yok olmasında veya değişmesinde failin taksir derecesinde dahi bir kusurunun bulunmadığı durumlarda, üçüncü fıkra hükmü değil, birinci fıkra hükmü uygulanacaktır[141].

Unutulmamalıdır ki, failin buradaki kastı sadece bilişim sistemine erişmek ve burada kalmak yani TCK'nın 243 (1) maddesini ihlal etmektir. Şayet fail, bilişim sistemine hukuka aykırı olarak erişip kasten verileri yok eder veya değiştirirse, artık tatbik edilecek hüküm, ayrı bir suç olan TCK'nın 244 (2) olacaktır[142].

Burada, verinin yok olması veya verinin değişmesi seçimlik sonuçlardır[143]. Bunlardan herhangi birinin meydana gelmesi cezayı artıran halin uygulanması için yeterlidir[144]. Ancak burada önemli olan, failde sistemdeki verileri yok etme yönünde bir kasıt bulunmamasıdır[145].

Madde metnindeki ifadeleri açıklamak gerekirse; verilerin yok edilmesi, tekrar ele geçirmenin imkansız ya da çok zor olmasına sebep olmak olarak değerlendirilebilirken verilerin değiştirilmesi nispeten daha sınırları belirsiz bir kavramdır. Verilerin değiştirilmesini de, bir yerden başka bir yere almak olarak değerlendirmemek gerekir. Değiştirme kelimesinden anlaşılması gereken önceki özelliklerini yitirmesi, amacına uygun şekilde kullanılamaması sonucunu doğuracak şekilde tahrif edilmesidir[146].

Burada yok olması veya değişmesi gereken veriler, hukuka aykırı olarak girilen ve orada kalınmaya devam edilen bilişim sisteminde yer alan

---

141 Benzer görüş ve açıklamalar için bknz. **Yaşar/Gökçan/Artuç**, s. 6747.

142 Benzer görüş ve açıklamalar için bknz. **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4634; **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 85; **Doğan,** s. 299; **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 904; **Malkoç,** s. 1671, 1672; **Karagülmez,** s. 175; **Çekiç,** s. 100; **Yenidünya,** s. 769; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 262; **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4654; **Esen** s. 630; **Tepe,** s. 281; **Soyaslan**, s. 613; **Parlar,** s. 19; **Koca,** s. 96; **Yaşar/Gökçan/Artuç**, s. 6769.

143 **Taşkın,** Bilişim Suçları, s. 37; **Karagülmez**, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, s. 176.

144 **Karagülmez,** Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, s. 176.

145 **Taşkın,** Bilişim Suçları, s. 37.

146 **Pallı,** s. 155. Benzer açıklamalar için bknz. **Yaşar/Gökçan/Artuç**, s. 6748.

verilerdir. Bunlar sistemin çalışmasına yarayan yazılımları oluşturan veriler olabileceği gibi, her hangi bir bilgi içeriğine ait veriler de olabilir[147].

Doktrinde hiçbir zarar doğmaksızın sadece verinin değişmesinin veya verilerin tamamen değişmesi ile kısmen değişikliğe uğraması arasında bir ayrım yapılmadan yaptırım altına alınmasını yerinde bulunmamış[148] ise de; biz böyle bir ayrımın gerekli olmadığına inanıyoruz. Zira, verinin tahrip boyutuna göre hakim cezayı tayin ederken pekala TCK'nın 61 (1) 'inci maddesindeki *"e) meydana gelen zarar veya tehlikenin ağırlığını", "f) Failin kast veya taksire kusurunun ağırlığını"* kriterleri gereği alt sınırdan uzaklaşabilecektir.

AKSSS'nin 2'nci maddesinde düzenlenen hukuka aykırı giriş suçunda netice sebebiyle ağırlaşan bir düzenlemeye yer verilmemiş olunması nedeniyle 243 (3) maddesinin sözleşmeyle çeliştiği görülmekteyse de, belirtmek gerekir ki, kanun koyucunun bilişim suçları alanında kaynak aldığı Fr. CK'nın 323-1 maddesinde de hukuka aykırı erişim sebebiyle bilişim sisteminin zarar görmesi hali cezayı artıran hal olarak düzenlenmiştir.

3.2. Manevi Unsur

Maddede saike işaret eden bir ibare bulunmadığından genel kast yeterlidir[149]. Bu suçtaki genel kast, failin bilişim sisteminin bir başkasına ait olduğunu ve bu kimsenin bu sistemin bütününe veya en azından bir kısmına girilmesini yasakladığını bilmesine rağmen, oraya girip kalmayı istemesini içermektedir. Bunlardan birisi, gerçekleşmez ise anılan suç manevi unsuru yönünden oluşmayacaktır.

---

147 **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 85.
Benzer açıklamalar için bknz. **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 263.

148 Recep Yılmaz **Yazıcıoğlu**, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt:II, Sayı:2 Yıl 2005, s. 408.

149 Benzer görüş için bknz. **Kurt,** s. 159; **Karagülmez**, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, s. 172; **Taşdemir**, Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 260; **Dülger**, Bilişim Suçları, s. 220; **Eker**, s. 123; **Esen,** s. 629; **Soyaslan,** s. 611; **Yenidünya,** s. 1037.

Failin bir bilişim sistemine hak sahibinin rızası dışında girerek burasının sınırlandığını görüp hemen çıkması durumunda, kastın isteme unsuru gerçekleşmediğinden, bu suç oluşmayacaktır[150].

TCK'nın 243 ve 244'üncü maddelerinde bu suçların sadece kasten işlenebilir şekilde düzenlenmiş olması AKSSS ile de uyum içerisindedir. Bu suçların kasten işlenebilir suçlar olması, özellikle servis sağlayıcıların kasten iştirak etmedikçe bu suçlardan dolayı sorumlu tutulmamasını sağlamaktadır[151].

Özel kast aranmaması nedeniyle failin merak, eğlence ya da oyun saiki ile hareket etmiş olması suçun oluşumu bakımından önemli değildir. Zaten madde gerekçesinde de sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının öneminin olmadığı vurgulanmıştır[152].

Doktrinde bir görüşe göre[153], failin özel bir saikle hareket etmesi aranmadığından bu suçun olası kastla da işlenebileceğinin kabulü gerekir. Bu durumda TCK'nın 21 (2)'inci maddesi uyarınca uygulama yapılır. Ancak doktrinde ki diğer görüşe göre[154], bu suçun tanımında fiilin hukuka aykırılığına özellikle işaret edildiğinden sadece doğrudan kastla işlenebilir. Kanaatimizce bu suçun oluşabilmesi için girmenin yanında sistemde kalmanın da şart olması nedeniyle olası kastla işlenmesi zaten mümkün değildir. Zira, olası kastla sisteme girilebilir ise de sistemde olası kastla kalınamaz. Örneğin yeteneklerini denemek için kendi geliştirdiği programla bilişim sistemlerine girmeye çalışan kişi, bunu başarırsa artık ya sistemden hemen

---

150 Necati **Meran**, Yeni Türk Ceza Kanunu'nda Sahtecilik - Malvarlığı - Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Ankara, Seçkin Yayınevi, 2005, s. 567.

151 **Doğan**, s. 297.

152 Benzer açıklamalar için bknz. Recep **Gülşen,** "İnternet ve Suç", İnternet ve Toplum, Editör, Ahmet **Tarcan**, Ankara, Anı Yayıncılık, 2005, s. 209; **Artuk/Gökçen/ Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4639; **Yenidünya**, s. 1037.

153 **Artuk/Gökçen/Yenidünya,** Türk Ceza Kanunu Şerhi, s. 4652; **Yaşar/Gökçan/Artuç,** s. 6746; **Karagülmez,** s. 172; **Kurt**, s. 151; **Doğan,** s. 297; **Koca,** s. 94; **Yenidünya,** s. 1037.

154 Mehmet Burak **Kızıltan**, "5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları", İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, yayınlanmamış yüksek lisans tezi, 2007, s. 68.

çıkacak ya da kasten kalmaya devam edecektir. Yani bu gibi durumlarda olası kast eklenen doğrudan kastla doğrudan kasta dönüşmüş olacaktır.

Bu madde bakımından dikkati çeken diğer husus ise, taksirli eylem neticesinde bir bilişim sistemine hukuka aykırı olarak girilmesinin veya bu fiil neticesinde sisteme zarar verilmesinin cezalandırılıp cezalandırılmayacağı hususudur. Bu madde çok rahatlıkla taksirle de işlenebilecek bir fiili cezalandırmaktadır. Ancak hem 765 sayılı hem de 5237 sayılı TCK sisteminde bir suçun taksirle işlenebiliyor olması istisnai durumdur ve cezalandırılabilme bakımından kanuni açıklık gerektirir. Bu madde metninde taksirle bir bilişim sistemine hukuka aykırı olarak girmenin suç olarak kabul edileceğine dair hüküm bulunmamaktadır. Bu nedenlerle failin taksirle bir bilişim sistemine hukuka aykırı olarak girmesi suç olarak kabul edilemez[155].

Doktrinde bir görüşe göre[156], failin bir bilişim sistemine tesadüfen girip buranın sınırlanmış olduğunu fark etmesine karşın burada kalmaya devam etmesi halinde, sonradan oluşan kast nedeniyle, TCK'nın 243'üncü maddesinde düzenlenen suç gerçekleşmiş sayılacaktır. Bu görüşe göre, taksirle veya bilmeden de olsa sisteme girmek "hukuka aykırı olarak girme" dir. Böylece girdiğini fark eden kişinin kalmaya devam etmesi ile suç oluşacaktır. Ancak suçun taksirli şekli düzenlenmediğinden bilmeden giren failin, durumu fark ettikten sonra makul bir sürede çıkması, suç kastının olmadığını ve hatayı (TCK. mad. 30) gündeme getirecektir. Kanaatimizce bu görüşe katılmak mümkün değildir. Zira madde metninde taksirli eylemin cezalandırılacağı açıkça belirtilmedikçe o eylemden dolayı kişilere ceza verilemez. TCK'nın 243'üncü maddesinde ise suçun oluşumu için açıkça genel kastla girme ve orada kalma aranmaktadır. Diğer bir değişle girme konusunda da bilme ve isteme unsuru aranmaktadır. Bu durumda taksirle giriş halinde girme hukuka aykırı olmadığından tipiklik açısından suç gerçekleşmemiş

---

155 **Doğan,** s. 298. Benzer açıklamalar için bknz. **Yaşar/Gökçan/Artuç**, s. 6745; **Karagülmez,** s. 172; **Kızıltan,** s. 68; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 260; **Gülşen,** s. 209; **Yenidünya/ Değirmenci,** s. 75, 76; **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 84; **Soyaslan,** s. 611; **Yenidünya,** s. 1037.

156 **Esen**, s. 629; **Yaşar/Gökçan/Artuç,** s. 6745, 6746; **Malkoç,** s. 1668,1669; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 260.

olacaktır. Kanaatimizce burada kanun koyucu istemeden taksirle girip ancak sonra sistemde kalınması halini de ayrıca müeyyide altına almalıdır[157].

Mukayeseli hukukta yetkisiz erişim açısından saike önem veren kanunlara rastlanmaktadır. Örneğin; 1991 tarihli Portekiz Bilişim Suçları Kanunu m.7/1'de yetkisiz olarak kendisine veya başkasına bir menfaat veya hukuka aykırı bir yarar elde etmek için her ne suretle olursa olsun bir sisteme veya bilişim ağına erişen kimsenin cezalandırılacağı hükme bağlanmıştır[158].

3.3. Hukuka Aykırılık Unsuru

Hukuka aykırılık, işlenen ve kanundaki tarife uygun bulunan fiile hukuk düzenince cevaz verilmemesi, bu fiilin mübah sayılmaması, yalnız ceza hukuku ile değil bütün hukuk düzeni ile çelişki ve çatışma halinde bulunması demektir[159]. Suç tipinde hukuka aykırılığın ayrıca belirtilmesine "hukuka özel aykırılık" denir. Kanun koyucu hukuka aykırılık unsurunu suç tipinde ayrıca göstererek; failin kanunun öngördüğü şekilde hareket ettiğini bilmesini ve hareket etmeyi istemesini aramaktadır. Diğer bir değişle, hukuka özel aykırılık halinin suç tipinde yer aldığı durumlarda hakim, failin kastı dışında ayrıca bu özel aykırılığı da bilip bilmediğini, buna göre hareket etmeyi isteyip istemediğini araştırmak zorundadır. Failin hukuka aykırı hareket ettiğini bildiği tespit edilmedikçe hukuka aykırılık unsuru ve dolayısıyla suç oluşmayacaktır[160].

---

157 Benzer görüş için bknz. **Biçkin**, s. 153.

158 Kanun metni için bkz. Stein **Schjolberg**, www.mossbyrett.of.no/info/legal.html 19.12.2005, Aktaran, Artuk/Gökçen/Yenidünya, Türk Ceza Kanunu Şerhi, s. 4652.

159 Ceza kanununun suç saydığı bir fiilin işlenmesine diğer bir hukuk kuralı –bu kural ceza kanununda veya başka bir hukuk dalına ait kanunda yer alabilir- izin veriyorsa, o fiilin hukuk düzeni tarafından yasaklanmadığı, yani suç olmadığı sonucuna ulaşılır. Bu şekilde ceza kuralının yasakladığı bir fiilin işlenmesine izin vererek, onun hukuka aykırı olmasını önleyen kurala "hukuka uygunluk sebepleri" denir. Hukuka uygunluk sebepleri, hukuka aykırılığı ortadan kaldırıp fiili hukukun meşru saydığı bir hareket haline getirirler. TCK'nın "Ceza Sorumluluğunu Kaldıran ve Azaltan Nedenler" başlıklı ikinci bölümünde "Hukuka Uygunluk Sebepleri" ve "Kusurluluğu Ortadan Kaldıran ve Azaltan Sebepler" bir arada düzenlenmiştir. TCK'nın da yer alan hukuka uygunluk sebepleri; kanun hükmünü yerine getirme yani görevin ifası (m.24/1), meşru savunma (m.25/1), hakkın icrası (m.26/1) ve ilgilinin rızası (m.26/2) yer almaktadır (**Artuk/Gökçen/Yenidünya**, Ceza Hukuku Özel Hükümler, s. 53 ve 55, 56).

160 **Artuk/Gökçen/Yenidünya**, Ceza Hukuku Özel Hükümler, s. 701, 702.

İnceleme konusu suçla ilgili ilk hukuka uygunluk sebebi, ilgilinin bilişim sistemi üzerinde hak sahibi olan kişi veya kişilerin, failin bu sisteme girmesi ve kalması konusunda sakatlanmamış bir rızalarının bulunmasıdır. Bir kimsenin failin bilişim sistemine girmesine ve orada kalmasına rızası var ise, bu durumda, artık suç oluşmayacaktır. Bu rıza açık olabileceği gibi zımni şekilde verilmiş bir rıza da olabilir[161]. Normal olarak aralarında ilişki bulunmayan bir kişinin başkasının sistemine girmesinde rıza ve onayının bulunmadığı kabul edilmelidir. Böyle bir durumda sisteme giren, rızanın varlığını ispat etmek durumundadır. Rızanın bulunduğu hallerde de bunun sakatlanmamış bir irade ürünü olması aranacak, iradeyi sakatlayan nedenlerin (hata, hile, cebir, korkutma) varlığı halinde rızanın varlığından söz edilemeyecektir[162]. Diğer bir değişle fail bir bilişim sistemine, sahibi ya da zilyedinin haberi olmaksızın girmiş ve orada kalmaya devam etmiş ise, mağdur olan, söz konusu girişin rızaya dayalı olarak gerçekleşmediğini değil, fail girişinin rızaya dayalı olarak gerçekleştiğini ispat etmek durumundadır[163].

Bazen hak sahibi failin bilişim sisteminin bir kısmına girmesine veya sistemdeki bazı şeyleri görmesine rıza göstermiş olabilir, bu durumda fail, kendisine izin verilen alanlar dışına girdiğinde bu rızaya aykırı davranmış olacak, dolayısıyla suç da oluşacaktır. Hak sahibinin rızasının olup olmadığı olaysal olarak değerlendirilecektir. Örneğin; bir gazete, kendi internet sitesine günlük gazetenin birinci sayfasını koymuş ve girişi herhangi bir şekilde engellememiş ise, bu durumda, aleni olarak herkese bu siteye girme konusunda izin verilmiş sayılır, rıza belli olmayan sayıdaki kimseye gösterilmiş olduğundan buraya girme hukuka aykırı sayılmayacaktır[164].

Burada vurgulamalıyız ki, rıza bilişim sistemi üzerinde hak sahibi olan kimse tarafından verilmelidir. Örneğin; bir bankanın personeline sisteme girebilmesi için şifre verdiğini, ancak bu personelin şifreyi bankayla ilgisiz

---

Benzer yönde açıklamalar için bknz. **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 84; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 259; **Dülger,** Bilişim Suçları, s. 219; **Doğan,** s. 296; **Yenidünya,** s. 1038; **Soyaslan,** s. 611.

161 **Yaşar/Gökçan/Artuç**, s. 6747.

162 **Malkoç,** s. 1666.

163 **Kurt,** s. 156.

164 **Yaşar/Gökçan/Artuç**, s. 6747. Benzer açıklamalar için bknz. **Akıncı,** s. 15.

bir kişiye verdiğini, şifreyi alan kişinin de sisteme girdiğini düşündüğümüzde, sisteme giriş için gerekli rıza yetkili kimse tarafından verilmediğinden şifreyi alan kişinin sisteme girmesi suç olacaktır[165].

Bir sisteme girme konusunda şifrenin konulmamış olması, rıza olduğu anlamını taşımaz. Örneğin, bir kimse komşusuna bilgisayarı kendi evine bırakması için verse, o kişide şifre içermeyen bilgisayarı açsa, bu durumda rızaya aykırı hareket mevcut olduğundan anılan suçun oluştuğu kabul edilecektir[166].

Suç şikayete bağlı olmadığından, mağdurun rızası eylem öncesinde elde edilmiş olmalıdır. Eylem sonrası onaylama, şikayetçi olmama, oluşan suçu ortadan kaldırmaz ve oluşan, suçun soruşturması ve kovuşturmasını engellemez[167].

Burada tartışılması gereken konulardan birisi de; mağdurun rızasıyla sisteme girildikten sonra, mağdurun rızasını kaldırmasına rağmen failin sistemden çıkmaması halinde suçun oluşup oluşmayacağıdır. Doktrinde bir görüşe[168] göre bu durumda da suç oluşacaktır. Bizimde katıldığımız diğer görüşe[169] göre ise, bu durumda suç oluşmayacaktır. Zira madde metninde suçun oluşması için "girme ve orada kalmaya devam etme" aranmaktadır. Öyle olunca failin mağdurun rızasına aykırı olarak bilişim sistemine girmesi ve yine rızaya aykırı olarak orada kalmaya devam etmesi gerekir. Bu nedenle burada girme safhasında mağdurun rızası bulunduğundan artık çıkmama ile anılan suç oluşmayacaktır, çünkü bu suç ancak her iki hareketin hukuka aykırı olarak gerçekleştirilmesi ile işlenebilen bir suçtur.

Bilişim sisteminin sahibinin rızası olmaksızın failin sisteme girdiği ve orada kaldığı sırada, sistem sahibi rıza verirse ne olacağı sorusunu cevaplamak gerekirse, kanaatimizce bu suçun mütemadi bir suç olması nedeniyle temadi devam ettikçe suç işlenmeye devam ediliyor demektir ve verilecek rıza eylemin hukuka aykırılığını kaldıracaktır[170].

---

165 **Taşdemir,** Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları, s. 259.

166 İsmail **Ergün**, s. 90.

167 **Malkoç,** s. 1667. Benzer açıklamalar için bknz. **Dülger,** s. 220.

168 **Kurt**, s. 92.

169 **Yaşar/Gökçan/Artuç**, s. 6747.

170 Benzer açıklamalar için bknz. **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 906.

Yasanın verdiği yetkiye dayanılarak izinsiz şekilde bilişim sistemine girilmesi ve orada kalınmaya devam edilmesi diğer bir hukuka uygunluk sebebidir. Bunun yanında CMK'nın 134'üncü maddesinde düzenlenen "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 gösterilen şartlara uygun olarak uygulanması halinde, kanun hükmünün icrası hukuka uygunluk sebebi nedeniyle de bu suç oluşmayacaktır[171].

Burada kamu görevlilerine çalıştıkları kurumlar tarafından verilen bilgisayarların, kurumun yetkili amiri veya teftişle görevli kişisi tarafından alınıp, el konulması ve içeriğine girilmesi hususuna da değinmekte fayda vardır. Bir defa bu bilgisayarların veriliş amacının iyi irdelenmesi gerekir, anılan bilgisayarlar özel işlerde değil, kurum işlerinde kullanılmak üzere verilmektedir, idare de verdiği veya tahsis ettiği bu bilgisayarları, yetkili merciin emri ile her zaman geri alabilir; alırken de bu bilgisayarların içinde kişiye özel bir veri bulunamayacağından, aksi durum 657 sayılı DMK'ya göre, kurum araçlarının özel işlerde kullanılması disiplin suçunu oluşturacağından, cihazın içeriğinin incelenmesi için de anılan kimsenin rızasına muhtaç olunmadığı kanaatindeyiz. Bu nedenle, kurum tarafından personeline verilmiş veya kullanımına tahsis edilmiş bilgisayarların, yetkili amir veya onun adına hareket eden kimsenin emri ile incelenmesinin hukuka aykırılık oluşturmayacağını düşünmekteyiz[172].

Bilişim sistemleri üzerinde meşru savunmanın[173] mümkün olup olmadığı konusunda kanaatimizce saldırının niteliğine bakılarak karar verilme-

---

171 **Doğan**, s. 297. Benzer açıklamalar için bknz. **Özbek/Kanbur/Doğan/Bacaksız/ Tepe**, s. 6747.

172 **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 6747.

173 Meşru savunmanın şartları;

1. Saldırıya ilişkin şartlar

a. Bir saldırının bulunması

b. Saldırının haksız olması

c. Saldırının bir hakka yönelmiş olması

d. Saldırının halen mevcut olması

2. Savunmaya ilişkin şartlar

a. Savunmada zorunluluk olması

lidir. Şayet saldırı ağ üzerinden yapılıyorsa, yapılan saldırı devam ederken saldırının mağdur tarafından anlaşılması halinde bilişim sistemi kapatıldığında, ya da en azından ağ bağlantısı kesildiğinde otomatik olarak saldırı da engellenmiş olunacağından meşru savunma mümkün olmayacaktır. Zira savunma yaparken karşı saldırı için zorunluluk bulunmamaktadır. Ancak sisteme fiilen temasla saldırı yapılıyorsa artık diğer şartlarının da bulunması halinde meşru savunma mümkündür.

Sonuç olarak; hukuka uygunluk halleriyle bilişim sistemine girilir ve orada kalınmaya devam edilirse, kanundaki maddi tanıma uyan bir fiil bulunsa dahi suç gerçekleşmeyecektir.

Mukayeseli hukukta da[174] inceleme konusu suçla ilgili olarak örneğin; Belçika CK. (m.550(b)) "yetkisiz olarak", Kanada CK. (m.342.1) "açık bir hakkı olmaksızın", Şili Otomatik Bilgi İşlem Suçları Kanunu (m.2) "hukuka aykırı olarak", Danimarka CK. (m.263) "hukuka aykırı" ibarelerine yer vererek hukuka özel aykırılığa işaret etmiştir[175].

AKSSS'de de bilişim suçlarının tümü için hukuka aykırılık unsurunun suç tipinde gösterilmesi ilkesini benimsemiştir. Sözleşmeye ilişkin açıklayıcı raporda, hak sahibinin rızası (örneğin; sistemin test edilmesi veya korunması için gerçekleştirilen erişimler), kamunun ücretsiz ve açık erişimine izin verilen bilişim sistemlerine girilmesi veyahut internette bir bilgiye ulaşmak için kullanılan standart erişim yöntemleri, bilişim sistemine hukuka aykırı girmek sayılmaz[176].

---

b. Savunmanın saldırıya ve saldırana karşı yapılması

c. Savunmanın tecavüz ile orantılı olması

174 Bkz. **Schjolberg,** www.mosstingrett.no/info/legal.html

175 **Artuk/Gökçen/Yenidünya,** Türk Ceza Kanunu Şerhi, s. 4653; **Artuk/Gökçen/Yenidünya**, Ceza Hukuku Özel Hükümler, s. 702; **Yenidünya,** s. 1038.

176 Bkz. Council of Europe - Explanatory Report to the Convention on Cybercrime (ETS No: 185), http//www.conventions.coe.int/Treaty/en/reports/Htm/185.htm (19.12.2005). tercüme edip aktaran, **Artuk/Gökçen/Yenidünya,** Türk Ceza Kanunu Şerhi, s. 4653. Benzer açıklamalar için bknz; **Doğan,** s. 297.

4. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

4.1. Teşebbüs

Sisteme hukuka aykırı olarak girip orada kalmaya devam etmekle suç tamamlanır[177].

TCK'nın 243'üncü maddesinin teşebbüse elverişli olup olmadığı, elverişli ise hangi safhadan sonra teşebbüsün söz konusu olacağı hususları doktrinde tartışmalıdır.

Doktrindeki bir görüşe[178] göre, bu suçta teşebbüs mümkün değildir. Zira bu suç birden fazla hareketlidir ve kalma hareketi parçalara bölünemediğinden teşebbüs mümkün değildir. Yasada maddi unsur olarak sisteme girmenin ve sistemde kalmaya devam etmenin cezalandırılmasını aradığından, her somut olayda da sistemde kalış süresi farklı şekilde yorumlanabileceğinden, hatta benzer olaylarda, yargıçların yorum farkı nedeniyle failin biri tamamlanmış suçtan, diğeri teşebbüsten ceza alabileceğinden adil olmayan sonuçlara yol açabilecektir. Dolayısıyla suç, failin sisteme girmesi ve çok kısa süreliğine de olsa sistemde kalmasıyla tamamlanmış olacağından, bu suçta teşebbüs uygulanmamalıdır.

Doktrindeki diğer görüşe[179] göre ise; bu suçta teşebbüs mümkündür. Ancak bu görüşte olan yazarlarda teşebbüsün olabileceği vakit konusunda farklı düşünmektedirler. Bazı yazarlara göre, bu suç birleşmiş hareketli suçtur ve birleşmiş hareketli suçlarda teşebbüsten söz edebilmek için ilk hareketin yapılması ardından ikinci harekete yönelik icra hareketlerinin de başlaması gerekir. Bu nedenle şayet sisteme girme hareketi gerçekleştirilemezse teşebbüsten de söz edilemez. Bu görüşte olan yazarlara göre her olayda kalınan süreye göre eylemin teşebbüs aşamasında mı yoksa tamamlanmış mı olduğunu hakim takdir edecektir[180]. Burada ölçü sürenin bilgileri

---

177 **Nurullah Aydın**, s. 382.

178 **Ketizmen**, s. 108; **Taşkın,** Bilişim Suçları, s. 30; **Parlar,** s. 18.

179 TCK'da 765 s. TCK'da yapıldığı şekli ile eksik-tam teşebbüs ayrımı yer almamaktadır. TCK gereği teşebbüs aşamasında kalan suçlarda failin alacağı cezanın belirlenmesinde, engel halin ortaya çıktığı anda failin icra hareketlerini tamamlayıp tamamlamamış olması değil, o ana kadar meydana gelen zarar ve tehlikenin ağırlığı dikkate alınacaktır. **Doğan**, s. 299.

180 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 465; **Taşkın,** "Bilişim Hukuku Uluslararası Uyuşmazlıklar", s. 334; **Özbek/Kanbur/Doğan/Bacaksız/Tepe,** s. 907; **Karagülmez,** s. 171; **Yenidünya,** s. 1039.

elde etmeye yetecek kadar olmasıdır[181]. Sadece sisteme girmeye çalışılması ya da anlık olarak sisteme girilip hemen çıkılması halinde teşebbüs söz konusu olamayacaktır[182]. Yasadışı erişimi sağlamış olmasına rağmen elektriklerin kesilmesi, sistemin kilitlenmesi vb. sebeplerle temadi teşkil edebilecek bir süre orada kalamayan ve bilişim siteminden çıkan failin suçu teşebbüs aşamasında kalmış olacaktır.

Bu suçta teşebbüs olabileceğini kabul eden diğer bir kısım yazara göre ise, failin elinde olmayan nedenlerle icra hareketlerine başlamasına rağmen eylemini tamamlayamaması durumunda suça teşebbüs gerçekleşmiş olacaktır. Bilişim sistemine girmek için gerekli işlemlerin yapıldığı örneğin; sistemin şifrelerinin kırılmaya çalışıldığı sırada teknik bir arızanın meydana gelmesi ya da sistemin kullanıcısı tarafından kapatılması gibi durumlarda, faile suça teşebbüsün düzenlendiği maddedeki orana göre cezası azaltılarak verilecektir[183].

Burada kabul edilecek görüşe göre gönüllü vazgeçme[184] kurumunun tatbikide değişecektir. Şayet bu suçların teşebbüse elverişli olmadığını kabul eden görüşü benimsersek girmeye çalışıldığı sırada vazgeçerse gönüllü vazgeçme tatbik edilebilecektir. Zira girmeyle eylemde tamamlanmış olacaktır[185]. Şayet bu suçun teşebbüse elverişli olduğunu kabul eden görüşü benimsersek; buradaki birinci grup yazarın görüşünü kabul ettiğimizde, fiil birleşik hareketli olduğundan gönüllü vazgeçme için giriş yetmez; kalmaya başladıktan sonra ancak eylem tamam oluncaya kadarki kalma da dolmadan sistemden çıkılması halinde gönüllü vazgeçme söz konusu olabilecektir.

---

181 **Taşkın,** "Bilişim Hukuku Uluslararası Uyuşmazlıklar", s. 334.

182 **Dalkılıç**, s. 220.

183 **Kurt,** s. 262. Benzer açıklamalar için bknz. **Esen** s. 631; **Taşdemir**, Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 260; **Malkoç**, s. 1669; **Nurullah Aydın**, s. 382; **Soyaslan,** s. 611; **Dülger,** Bilişim Suçları, s. 221.

184 Gönüllü vazgeçme

Madde 36- (1) Fail, suçun icra hareketlerinden gönüllü vazgeçer veya kendi çabalarıyla suçun tamamlanmasını veya neticenin gerçekleşmesini önlerse, teşebbüsten dolayı cezalandırılmaz; fakat tamam olan kısım esasen bir suç oluşturduğu takdirde, sadece o suça ait ceza ile cezalandırılır.

Gönüllü vazgeçme kurumu hakkında ayrıntılı bilgi için bknz. **Yavuz Erdoğan**, "Gönüllü Vazgeçme", Ceza Hukuku Dergisi, Yıl:5, Sayı:13, Ağustos 2010, s. 93 vd.

185 **Taşkın,** Bilişim Suçları, s. 30.

Zira, bu görüşe göre sisteme giriş tek başına suç oluşturmamaktadır. Şayet ikinci görüşte olup ancak ikinci grubun görüşünü benimsersek, diğer bir değişle giriş için yapılan hareketler safhasında da teşebbüsün olabileceğini kabul eden görüşü benimsersek bu durumda artık giriş safhasındaki vazgeçmelerde de gönüllü vazgeçme tatbik edilebilecektir.

Kanaatimizce bu suçlara teşebbüs mümkündür. Ancak suçun oluşması için birden fazla hareket gerektiğinden girme tamamlanmadıkça teşebbüs söz konusu olamaz. Diğer bir değişle, biz ikinci görüşün birinci grubunun fikirlerini destekliyoruz. Ayrıca belirtmeliyiz ki, girdikten sonra eylem tamamlanmadan rızayla çıkılması halinde teşebbüs hükümlerinin değil gönüllü vazgeçme hükümlerinin tatbiki gerekir.

Kabulümüzün sonucu olarak, fail sisteme bilfiil girmeden elektronik posta yoluyla mağdura truva atı programı[186] gönderse, mağdur bu programı sistem içine alsa, program kendisini sistem dosyalarına kopyalasa, truva atını sisteme yerleştiren şahıs sistem içine henüz girmediğinden suç gerçekleşmeyecektir. Ancak, söz konusu truva atı özelliği taşıyan program vasıtasıyla sisteme girdiği ve kalmaya devam ettiği takdirde suç gerçekleşecektir. Özellikle bu son halde truva atı özellikli program posta yoluyla bir başka programın veya ses dosyasının uzantısı olarak kamufle edilmiş tarzda birisine gönderilmektedir. Postayı alan kişi iletiyi kendi rızası ile açmakta fark etmediği zararlı yazılımı bilişim sistemine bizzat kendisi almaktadır. İleti açılır açılmaz bu iletinin eklentisi olarak gönderilen casus yazılım kendisini sistem değişik yerlerine gizli bir şekilde kopyalamaktadır. Görüldüğü gibi iletiyi gönderen şahıs burada bu safhaya kadar bilişim sistemine fiili olarak hiç girmemektedir. Ancak sistem içine değişik yöntemlerle sokulan casus program sayesinde fail her an sisteme ulaşabilir hale gelmekte, sistemin içinde her yapılan işlemi istediği takdirde izleme[187] imkanına kavuşmakta,

---

186 Truva atı, yararlı gibi görünen ancak aslında zarara yol açan bilgisayar programlarıdır. Truva atları, insanların, meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya yöneltilmeleri yoluyla yayılır. Mitolojideki Truva atı nasıl bir armağan gibi görünüp, aslında Troya kentini ele geçirecek Yunanlı askerleri taşıyorduysa; bugünün Truva atları da yararlı yazılımlar gibi görünen bilgisayar programlarıdır, ancak güvenliğinizi tehlikeye atar ve pek çok zarara yol açarlar (http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/76.html 16.05.2011). benzer açıklamalar için bknz. **Yılmaz,** "5237 Sayılı TCK'nın 244.Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", s. 75.

187 5651 s. Kanun'a dayanarak çıkarılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in tanımları açıklayan 3 (1) j) mad-

yani o sistem içine nüfuz edebilme imkanını elinde tutmaktadır. Bu imkanı sağlayacak unsurları, zararlı programları bu şekilde sisteme sokan ve orada bulundurmaya devam eden ancak sisteme hiç girmeyen ve bu arada da yakalanan bir şahsı fiilen sisteme girmediği için bu maddeye göre cezalandırmak mümkün değildir[188].

TCK'nın 243 (3)'üncü maddesinin neticesi sebebiyle ağırlaşmış hal olarak kabul edilir ise; neticesi sebebiyle ağırlaşmış suçlar hareket parçalara bölünmedikçe teşebbüse elverişli olmadıklarından dolayı[189] ve ayrıca taksirli suçlar da teşebbüse elverişli olmadıklarından dolayı bu durumda teşebbüs mümkün değildir[190].

Hükümet tasarısından farklı olarak[191] TCK'da bilişim alanında suçlarda suça teşebbüs halinde tamamlanmış suç gibi cezalandırma hükmüne yer verilmemiştir.

Bu suçun gerçekleşmesi için ayrıca bir zararın oluşması gerekmemektedir[192]. Bu nedenle bu bir tehlike suçudur[193]. Kanun, hukuka aykırı olarak girme ve orada kalmaya devam etmeyi suçun oluşması için yeterli saymakta olduğundan ayrıca hakim tarafından bu girme ve kalma neticesi verilerin güvenliğinin tehlikeye düşüp düşmediğini araştırmaya gerek bulunmaz. Bu sebeple girme ve kalma eyleminin gerçekleşmesi ile suç da

---

desinde izleme *"İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini ifade eder"* şeklinde tanımlanmıştır.

188 **Kurt,** s. 149.

189 Parçalara bölünebiliyorsa teşebbüs mümkündür.

190 Benzer açıklamalar için bknz. **Özbek/Kanbur/Doğan/Bacaksız/Tepe,** s. 907; **Yazıcıoğlu,** s. 86; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 260; **Yaşar/Gökçan/Artuç,** s. 6751.

191 Hükümet tasarısının 346 ncı maddesinin üçüncü fıkrasında ki *"Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir"* şeklindeki hüküm, 5237 s. TCK'nın 243 ncü maddesinde yer almamıştır.

192 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4634.

193 Eğer bir suçun oluşması için zarar meydana gelmesi aranıyorsa bunlara zarar suçu, buna karşılık suçun meydana gelmesi için zarar tehlikesinin doğması yeterli ise, buna da tehlike suçları denir. Zarar suçlarında korunan hukuki yarara zarar verilirken, tehlike suçlarında korunan hukuki yarar açısından sadece tehlike doğmaktadır. Bilindiği üzere tehlike suçları somut tehlike suçları ve soyut tehlike suçları diye ikiye ayrılmaktadır.

tamamlanmış sayılır yani bilişim sistemine girme suçunun birinci fıkrası soyut tehlike suçudur[194].

4.2. İştirak

Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalmaya devam etme fiili iştirak bakımından bir özellik taşımamaktadır. Dolayısıyla, suçta iştirak değerlendirilirken TCK'nın 37, 38, 39 ve 40'ıncı maddelerindeki düzenlemeleri dikkate alınacak ve olay buna göre değerlendirilecektir[195]. Anılan suç mütemadi suç olduğu için, temadi sona erinceye kadar anılan suça katılmak mümkündür[196].

Ayrıca belirtmek gerekir ki, yasadışı erişimin sağlanmasında erişim sağlayıcılar da, suç işleme kastı ve iştirak iradelerinin bulunması şartıyla, suça iştirakten sorumlu tutulabilecektir.

Bu suç bakımından söz konusu olabilecek iştirak şekilleri daha ziyade suçun işlenmesinde kullanılan araçları sağlamak ve suç işlemeye teşvik şeklinde olabilecektir. Örneğin; suçun işlenmesi için bir kimseye ihtiyacı olan bilgisayar ve unsurlarını tedarik eden veya kişiyi suç işlemeye teşvik eden kişi suça iştirak iradesinin de olması şartıyla iştirak hükümlerince yardım eden olarak (TCK m.39) cezalandırılabilecektir[197].

---

194 **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243 . Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 84.
Benzer açıklamalar için bknz. **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 903; **Doğan,** s. 295; **Malkoç,** s. 1669; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 257; **Ketizmen**, s. 79.
Nitekim suçun bir tehlike suçu olduğu maddenin gerekçesinde "*sisteme hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur"* denilmek suretiyle vurgulanmıştır.

195 **Taşkın,** Bilişim Suçları, s. 30, 31. Benzer açıklamalar için bknz. **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 86; **Yaşar/Gökçan/Artuç**, s. 6751; **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 907; **Dülger,** Bilişim Suçları, s. 222, 223; **Doğan,** s. 300.

196 **Yaşar/Gökçan/Artuç**, s. 6751.

197 **Doğan,** s. 300.

4.3. İçtima

TCK'nın genel gerekçesinde de belirtildiği üzere ceza hukukunda kural olarak kaç tane fiil varsa o kadar suç vardır. Bunun istisnası ise, suçların içtiması bölümünde belirtilen hususlardır. İçtimanın farklı şekiller vardır. Bunlar:

- TCK'nın 42'nci maddesinde düzenlenen işlenen suçun başka bir suçun unsuru ya da ağırlatıcı nedeni (cezayı artıran hali) olması hali (bileşik suç),
- TCK'nın 43 (1) maddesinde düzenlenen bir suç işleme kararıyla değişik zamanlarda ancak bir kişiye karşı aynı suçun birden fazla kez işlenmesi hali (zincirleme suç),
- TCK'nın 43 (2) maddesinde düzenlenen aynı suçun birden fazla kişiye karşı ancak tek bir fiille işlenmesi hali (zincirleme suç)
- TCK'nın 44'ncü maddesinde düzenlenen tek bir fiille birden fazla suçun işlenmesi hali (fikri içtima),

Suçların içtiması halinde cezalar içtima edilmemekte, tam tersine kanun koyucu bazı suçları cezalandırmaktan feragat etmektedir.

TCK'nın 243 (1) maddesinde düzenlenen bilişim sistemine girme suçu zorunlu olarak mütemadi bir suçtur[198]. Bu suç mütemadi suç olduğundan kalınan süre kesilmediği sürece ne kadar uzun olursa olsun tek suç olmaya devam edecektir. Kalınan sürenin uzunluğu TCK'nın 61'nci maddesi uyarınca temel cezanın belirlenmesinde nazara alınabilecektir[199].

Bu suç zincirleme suç hükümlerinin uygulanmasına elverişlidir. Yani, fail aynı suç işleme kararıyla bir kişiye ait bir bilişim sistemine değişik zamanlarda ancak makul zaman aralıklarıyla[200] birden fazla kez girip orada

---

198 **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 84.
Benzer açıklamalar için bknz. **Malkoç,** s. 1670; **Öngören,** s. 46; **Taşkın,** Bilişim Suçları, s. 31; **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 260-261.

199 **Yaşar/Gökçan/Artuç**, s. 6751; **Soyaslan,** s. 612.

200 Fail uzun zaman aralıklarıyla ya da her seferinde sistemdeki başka bir veriyi elde etmek için sisteme giriyor ve orada kalmaya devam ediyorsa failde aynı suç işleme kastının

kalırsa (TCK m.43 (1)) ya da tek bir eylemle birden fazla bilişim sistemine girip kalırsa (TCK m.43 (2)) zincirleme suç hükümleri uygulanacaktır. Ancak, farklı bilişim sistemlerine farklı fiillerle girilip orada kalmaya devam edilmesi halinde her bir bilişim sistemine girme ayrı bir suç olarak değerlendirilecek ve burada zincirleme suç hükümleri uygulanamayacaktır. Failin girip belli bir süre kaldığı bilişim sisteminin birden fazla kimseye ait olması halinde ise, zincirleme suç söz konusu olmayıp tek suç oluşacaktır. Ancak burada belirtmeliyiz ki bir kimsenin kişisel dosyasını arkadaşının bilgisayarında muhafaza ettiği hallerde, bu bilgisayara girilerek söz konusu dosyaya ulaşılması halinde, hem bilgisayarın sahibine hem de veri sahibine karşı suç işlenmiş olur. Bu ihtimalde diğer koşulları da varsa TCK. m.43/2 uygulanmalıdır[201].

Bilişim sistemine hukuka aykırı erişim ve sistemde kalmaya devam etme, bilişim sistemlerine girerek işlenmesi zorunlu bulunan başka bilişim suçlarının işlenmesi için de bir araçtır. Bu itibarla 243'üncü maddede yer alan suç, daha sonra işlenen bu suçlar bakımından bir geçit olma özelliği taşır[202]. Örneğin; TCK'nın 244'üncü maddesindeki bilişim sisteminde var olan verileri başka bir yere göndermek veya bir bilişim sistemindeki verileri değiştirmek ya da bozmak için sisteme girmek de gerekmektedir. İşte bu gibi durumlarda iki madde arasındaki içtima ilişkisinin nasıl olacağı bir sorun olarak karşımıza çıkmaktadır.

Doktrinde geçit suçu kurumunu kabul etmeyen bir görüş[203], burada failin kastına bakılarak tatbik edilmesi gereken maddenin belirlenmesi gerektiğini savunur. Buna karşı doktrinde burada geçitli suç kurumunu kabul eden pek çok yazar bulunmaktadır. Ancak geçitli suç kurumunu kabul eden yazarlar arasında konumuz itibarıyla görüş ayrılıkları bulunmaktadır. Bir görüş[204] sisteme girip kalmanın araç suç olduğunu, girişten sonra amaç suçun

---

varlığından söz edilemeyeceğinden fail her bir eylem ayrı ayrı cezalandırılmalıdır. Başka bir değişle, suçların değil, cezaların içtimai kuralı uygulanmalıdır.

201 Zincirleme suç bakımından içtima hususunda benzer açıklamalar için bknz. **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4655; **Dülger,** s. 225, 226; **Öngören,** s. 46; **Taşkın,** Bilişim Suçları, s. 32; **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 907, 908. **Esen,** s. 631; **Soyaslan,** s. 612.

202 **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4655; **Yenidünya**, s. 1039.

203 **Özbek/Kanbur/Doğan/Bacaksız/Tepe**, s. 908.

204 **Malkoç,** s. 1670.

gerçekleştirildiğini; bu durumda sisteme girip kalmanın amaç suçun unsuru ya da cezayı artıran hal olarak düzenlenip düzenlenmediğine bakmak gerektiğini, yapılacak tespitte şayet araç suçun yani sisteme girip kalmanın amaç suçun icra hareketi olarak amaç suçta yer alıyorsa artık amaç suçtan ceza verilmesi gerektiğini, şayet böyle bir durum yoksa gerçek içtima kuralları gereği her bir eylem bağımsız olacağından ayrı ayrı ceza vermek gerektiğini belirtirler. Bu görüşteki yazarlara göre sisteme girip kalma TCK'nın 132, 133, 134, 135, 142, 158, 244, 245'inci maddelerinde sisteme giriş suçun unsurlarından olan icra hareketlerinden sayılmadığından bu durumlarda faile hem 243 hem de diğer eylemden ayrı ayrı ceza vermek gerekecektir. Doktrinde diğer görüşe göre[205], burada 243 gerçekleşmeden amaç suç yapılamıyorsa yalnızca amaç suçtan dolayı ceza verilmelidir. Diğer bir değişle, bilişim sistemine girmeden suç işlenemiyorsa fail sadece neticeden sorumlu olmalıdır. Örneğin bilişim sisteminin işleyişini engellemek için bilişim sistemine girip kalan failin sadece TCK 244'üncü maddeden cezalandırılacağını belirtir. Bizimde katıldığımız bir diğer görüş[206], bu durumlarda fikri içtima kuralları uygulanmalı ve TCK'nın 124, 132, 244 gibi cezası daha ağır olan maddeleri tatbik edilmelidir. Bir diğer görüş[207] ise, kanun koyucu açıkça göstermese de 244'üncü maddedeki hal 244'üncü maddedeki fiillerin unsurunu teşkil etmektedir. Bu nedenle geçitli suç hükümleri uygulanıp iki ayrı ceza verilemez. Sadece final suç olan 244'üncü maddeden ceza verilmelidir.

Failin 243'üncü madde kapsamındaki genel kast ile bilişim sistemine yetkisiz girmesi ancak, kalmaya başlamadan sistemden çıkması sonucunda sistemin içerdiği veriler yok olması veya değişirse ne olacaktır? Kanaatimizce TCK'nın 243'üncü maddesinin temel şeklini düzenleyen ilk fıkrasında sisteme girmenin yeterli görülmeyip sistemde kalınmasının da aranması, tartışma konusu olayda ise sistemde kalınmaması nedeniyle suç maddi unsurları itibarıyla oluşmayacaktır[208]. Ancak, bu noktada belirtmeliyiz ki,

---

205 **Karagülmez,** s. 181. Benzer açıklamalar için bknz. **Artuk/Gökçen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4655; **Doğan**, s. 300.

206 **Koca,** s. 96; **Dülger**, Bilişim Suçları, s. 225.

207 **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 86.
Benzer açıklamalar için bknz. **Taşdemir,** Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, s. 261.

208 Benzer açıklamalar için bknz. **Karagülmez,** s. 176-178.

eylem suç olmasa bile burada mağdurun özel hukuka ilişkin hakları devam etmektedir. Bu verdiğimiz cevaptan sonra bu kez akla bedeli karşılığı bir girilebilen bir sisteme yetkisiz olarak girilmesi ve kast olmaksızın verilere zarar verilmesi halinde ne olacağı sorusu gelmektedir. Diğer bir değişle TCK'nın 243 (1), (2), (3) fıkralarının tamamının birden gerçekleşmesi halinde ne olacaktır? Kanaatimizce her ne kadar TCK'nın 61 (4) maddesinde bir suçun daha ağır ve daha az cezayı gerektiren birden fazla nitelikli halin gerçekleşmesi halinde önce artırma sonra indirme yapılacağı açıkça belirtilmiş ise de; inceleme konumuz olan durumda 243 (3) fıkrasında artırım oranı gösterilmeyip doğrudan ceza tayin olunması nedeniyle TCK'nın 61 (4) maddesinin burada tatbiki imkanı yoktur. Kaldı ki, ikinci fıkra düzenlenirken madde metninde "yukarıdaki fıkrada" denilmesi nedeniyle bu fıkranın üçüncü fıkra ile birlikte uygulanması suçta ve cezada kanunilik ilkesine de uymayacaktır. Bu nedenle kanaatimizce failin tek eylemle kanunun birden fazla hükmünü ihlal ettiği değerlendirilerek daha yüksek ceza öngören (mevcut tartışmada cezayı indirmeyip artıran) 243 (3) maddesi tatbik edilmelidir[209]. Ancak burada belirtmek zorundayız ki, biz TCK'nın 243 (3) maddesini neticesi sebebiyle ağırlaşan hal kabul ettiğimizden suçun unsurlarının tespiti bakımından artık TCK'nın 243 (1) maddesi tatbik edilmelidir.

5. YAPTIRIM

TCK'nın 243'üncü maddesinin birinci fıkrasında düzenlenen suçu işleyen kimse, 1 yıla kadar hapis veya adli para cezasıyla cezalandırılır. Burada maddede hapis cezasının alt sınırı belirtilmediğinden, cezanın alt sınırı TCK'nın 49 (1) maddesi uyarınca 1 aydır. Seçimlik ceza olarak öngörülen adli para cezasının alt sınırı ise, TCK'nın 61 (9) maddesinin[210] 5560 s. Kanun'la yürürlüğe girdiği 19.12.2006 tarihinden önce[211] işlenen suçlarda 5 gün, bu tarihten sonra işlenen suçlarda ise 30 gündür, adli para

---

209 Benzer açıklamalar için bknz. **Karagülmez,** s. 178.

210 (9) (Ek: 6/12/2006 - 5560/1 md.) Adlî para cezasının seçimlik ceza olarak öngörüldüğü suçlarda bu cezaya ilişkin gün biriminin alt sınırı, o suç tanımındaki hapis cezasının alt sınırından az; üst sınırı da, hapis cezasının üst sınırından fazla olamaz.

211 01.06.2005 - 19.12.2006 arası olup, 01.06.2005 tarihinden önceki suçlarda 765 s. TCK ile lehe kanun tartışması yapmak gerekmektedir.

cezasının üst sınırı da 19.12.2006 tarihinden önce işlenen suçlarda 730 gün iken, bu tarihten sonra işlenen suçlarda 365 gündür[212].

Bilişim sistemlerinin artık hayatımızın tamamını kuşatmış olması ve sosyal hayatın onun üzerine kurulu olması nedeniyle TCK'nın 243'üncü ve devamındaki maddelerde korunan hukuki değerlerde dikkate alındığında bu maddelerde bulunan cezalar yetersizdir. Cezaların biran evvel artırılması gerekmektedir[213]. Nitekim TBMM komisyonunda TCK'nın 243 ve 244'üncü maddelerinde belirtilen suçlarda cezaların artırılması için bir tasarı halen beklemektedir[214]. Sırası gelmişken belirtmek gerekir ki, TCK'nın 243 (1)'inci maddesinin tasarıdaki halinde ceza "iki yıla kadar hapis veya adli para cezası" olarak belirlenmiş iken TBMM Genel Kurulu'ndaki görüşmeler sırasında ceza "bir yıla kadar hapis veya adli para cezası" olarak değiştirilmiş; TCK'nın 243 (3) maddesindeki cezada "iki yıldan dört yıla kadar hapis cezasına" olarak belirlenmişken "altı aydan iki yıla kadar hapis cezasına" şeklinde değiştirilmiştir.

TCK'nın 243'üncü maddesi uyarınca hükmolunan ceza 2 yılı geçemeyeceğinden ceza hükmünün açıklanması, CMK'nın 231'inci maddesi uyarınca, geri bırakılabilir[215]. Hükmün açıklanmasının geri bırakılması kurumu tatbik edilmek istenmezse ya da şartları yoksa, hükmolunan hapis cezası TCK'nın 51'inci maddesi uyarınca ertelenebilir. Ayrıca belirtmek gerekir ki, 1 yıldan az hapis cezası verilmesi halinde, hapis cezası seçenek yaptırımlara da çevrilebilir.

Burada dikkat edilmelidir ki, TCK'nın 243 (1) maddesinde hakime hapis cezası veya adli para cezası verme konusunda takdir yetkisi tanınmış-

---

212 **Yaşar/Gökçan/Artuç,** s. 6752.

213 Benzer açıklamalar için bknz. **Yazıcıoğlu,** "Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi" s. 86.

214 Bknz. http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.sorgu_yonlendirme 08.04.2011.

215 Yargıtay 11.CD., 26.03.2008 gün ve 38-1789 esas ve karar sayılı ilamında özetle "Sanığın, katılan D.I'ya yönelik suçundan kurulan mahkûmiyet hükmüyle ilgili olarak, hükümden sonra 08.02.2008 günlü 26781 sayılı Resmi Gazete'de yayımlanarak aynı gün yürürlüğe giren ve sanık lehine sonuç doğuran 5728 sayılı Yasanın 562.maddesi ile değişik 5271 sayılı CMK.nun 231.maddesi gereğince, sanık hakkında "hükmün açıklanmasının geri bırakılması" kararının verilip verilmeyeceği hususunun tartışılmasında zorunluluk bulunması, bozmayı gerektirmiştir" denilmiştir (**Parlar,** s. 51).

ken[216] TCK'nın 243 (3) maddesinde mutlaka hapis cezası verilmesi gerektiği belirtilmiştir. TCK'nın 243 (2) maddesinde ise, 1'inci fıkradaki cezanın yarısına kadar indirileceği düzenlenmiştir. TCK'nın 243 (2) maddesinde hakimin takdir yetkisinin olmadığı mutlaka 1/2 oranında indirim yapması gerektiği yönünde doktrinde görüş[217] bulunmakta ise de; kanaatimizce kanun metninde "yarısına kadar indirilir" denilmesi nedeniyle hakimin daha az oranda indirim yapma konusunda pekala takdir hakkı bulunmaktadır.

Suç tanımında hapis cezası ile adli para cezasının seçenek olarak öngörülmesi dolayısıyla, hâkim hapis cezasını tercih ettikten sonra, bunu artık para cezasına çeviremez (TCK. m.50/2). Diğer tedbirlere hükmetme konusunda ise, bir sınırlama yoktur. Tekerrür halinde (TCK. m.58), adli para cezası ile hapis cezası seçimlik ise, hâkimin takdir yetkisi sınırlandırılmış olup, hâkim hapis cezasına hükmetmek zorundadır. Bu ihtimalde, kanımızca hapis cezasının adli para cezasına çevrilmesi olanaklıdır[218].

Fail başlığı altında incelediğimiz üzere, TCK'nın 20'nci maddesiyle tüzel kişilerin suçun faili olamayacağı açık bir şekilde düzenlenmiştir[219], ancak tüzel kişiler hakkında güvenlik tedbiri uygulanabilecektir[220]. Bu uygu-

---

216 TCK'nın 243 (1) maddesinde "veya" bağlacı kullanıldığından hakim iki cezaya birden hükmedemeyecektir.

217 **Yaşar/Gökçan/Artuç,** s. 6752.

218 **Yenidünya,** s. 1041.

219 CMK.nın "Tüzel kişinin temsili" başlıklı 249'ncu maddesi;

"Madde 249.- (1) Birtüzel kişinin faaliyeti çerçevesinde işlenen suçlardan dolayı yapılan soruşturma ve kovuşturmalarda tüzel kişinin organ veya temsilcisi, katılan veya savunma makamı yanında yer alan sıfatıyla duruşmaya kabul edilir.

(2) Bu durumda, tüzel kişinin organ veya temsilcisi bu Kanunun katılana veya sanığa sağladığı haklardan yararlanır.

(3) Birinci fıkra hükmü, sanığın aynı zamanda tüzel kişinin organ veya temsilcisi sıfatını taşıması halinde uygulanmaz." şeklinde olup tüzel kişilerin kamu davasında temsili hususu düzenlenmek suretiyle sistemin muhakeme hukuku bakımından işleyişine açıklık getirilmiş bulunmaktadır.

220 Anayasamızda da güvence altına alınan "ceza sorumluluğunun şahsiliği" kuralının gereği olarak sadece gerçek kişiler hakkında ceza yaptırımına hükmedilebilir. Ancak bu ilke, işlenen suç dolayısıyla özel hukuk tüzel kişileri hakkında güvenlik tedbiri niteliğinde yatırımlara hükmedilmesine engel değildir. Nitekim TCK'nın 20'nci maddesinin gerekçesinde bu hususla ilgili olarak; *"Özel hukuk tüzel kişilerinin suç faili sayılıp sayılmaması ile işlenen bir suçtan dolayı bunlar hakkında bir yaptırıma hükmedilmesi sorununu birbirinden ayırmak gerekir. Suç ve ceza politikası gereği olarak ancak gerçek*

lama, TCK'nın 60 (4) maddesi gereğince yalnızca yasada bunun açıkça belirtildiği hallerde olabilecektir. TCK'da bilişim alanında suçların düzenlendiği bölümün sonunda yer alan 246'ncı maddede "*bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur"* ifadesi yer aldığı için bu suçun işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlaması halinde bunlara TCK'nın 60'ıncı maddesindeki[221] kendilerine özgü güvenlik tedbirleri (iznin iptali ya da müsadere) uygulanacaktır[222].

Ancak unutulmamalıdır ki, aynı maddenin üçüncü fıkrası gereği, güvenlik tedbiri uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hakim bu tedbirlere hükmetmeyebile-

---

kişiler suç faili olabilir ve sadece gerçek kişiler hakkında ceza yaptırımına hükmedilebilir. Bu anlayış, Anayasamızda da güvence altına alınan ceza sorumluluğunun şahsiliği kuralının bir gereğidir. Ancak, işlenen suç dolayısıyla özel hukuk tüzel kişileri hakkında güvenlik tedbiri niteliğinde yaptırımlara hükmedilebilecektir" şeklinde açıklama yapılmıştır (**Parlar,** s. 201).

765 s TCK'da tüzel kişilerin bilişim suçlarından dolayı sorumlu tutulabileceğine dair herhangi bir hüküm bulunmamaktaydı. Tüzel kişilerin cezai eylemlerden sorumlu tutulması 5237 s. TCK ile ceza hukukumuza girmiştir (**Biçkin,** s. 165).

Yasalaşmayan Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısının 27'nci maddesi "Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması" başlığını taşımakta olup "Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 27 - (1) Bu Kanunun Üçüncü, Dördüncü ve Beşinci Bölümünde sayılan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur" şeklinde idi.

221 TCK'nın 60'ıncı maddesine göre tüzel kişilerin sorumlu tutulabilmesi için;

- Öncelikle bir özel hukuk tüzel kişisi söz konusu olmalı,
- Özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle işlenen bir suç söz konusu olmalı,
- Suç tüzel kişinin yararına işlenmiş olmalı,
- Suç kasten işlenen bir suç olmalı,
- Suçun yargılaması mahkumiyetle sonuçlanmış olmalı,
- Kanunun ilgili yerinde tüzel kişilere yaptırım uygulanabileceği açıkça düzenlenmiş olmalı (inceleme konumuz bakımından daha önce belirttiğimiz üzere TCK'nın 246'ncı maddesinde açıkça düzenlenmiştir),
- Ayrıca iznin iptali tedbirinin uygulanabilmesi için suçun iznin verdiği yetkinin kötüye kullanılması suretiyle işlenmiş olmalıdır.

222 **Dülger**, Bilişim Suçları, s. 229; **Avşar/Öngören**, s. 147.

cektir. Burada hakim takdirini kullanacaktır. Kanaatimizce bu fıkra oldukça isabetli bir düzenlemedir. Zira, tüzel kişiye uygulanacak yaptırımlar pekala olayla ilgisi olmayan kişi ya da kurumları da (örneğin; orada çalışanları) olumsuz etkileyebilecektir.

TCK.nun 60.maddesinde sözü edilen ve haklarında güvenlik tedbiri niteliğinde yaptırımlara hükmedilebileceği öngörülen tüzel kişiler "özel hukuk tüzel kişileri" dir. Bu itibarla kamu hukuku tüzel kişileri bu madde kapsamında değildirler. Bu nedenle kamu tüzel kişilerine güvenlik tedbiri uygulanması söz konusu olmayacaktır. Kanaatimizce kamu ya da özel hukuk tüzel kişisi ayrımı yapılması yerinde değildir. Zira örneğin bir belediyenin yaptığı eylemin aynısını başka bir belediyede taşeron olarak çalışan şirket yaptığında belediye bir yaptırımla karşılaşmamasına rağmen şirket karşılaşacaktır. Bu durum hakkaniyete aykırı olacaktır.

Bu noktada belirtmek gerekir ki, doktrinde[223] bu suçlarla tüzel kişi arasında uygun bir illiyet bağının kurulması için "haksız menfaat" ölçütünün yeterli olmadığı, AKSSS şerhinde de belirtildiği üzere bu babda bir cezai yükümlük doğması için sağlanması gereken şartlar arasında, suçun, tüzel kişinin yetkili bir yöneticisi yahut çalışanı, vekili tarafından yetkilerinin kullanılması sırasında işlenmesi ve haksız menfaat şartının eklenmesi gerektiği belirtilmiş ise de; kanaatimizce tüzel kişiler hakkında güvenlik tedbirlerini düzenleyen TCK'nın 60'ıncı maddesinde bu hususa zaten yer verildiğinden 246'ncı madde metninde böyle bir hususa yer verilmesi gereksiz tekrar olacaktır.

Kanaatimizce, tüzel kişilerin sorumluluğunun kabul edilmesi, AKSSS'de de belirtildiği üzere[224], bilişim suçlarıyla mücadele bakımından olması gereken bir düzenlemedir. Bu sorumluluğun cezai sorumluluk şeklinde düzenlenmemiş olması da isabetlidir. Zira tüzel kişilerin cezai sorumluluğunun kabul edilmesi, cezaların şahsiliği ilkesi ve kusursuz suç ve ceza

---

223 **Eker**, s. 131.

224 12'nci maddesin de Kurumsal Sorumluluğu kabul ederken bir takım koşulların gerçekleşmiş olmasını aramaktadır. Bunlardan en önemlisi anılan suçların tüzel kişiliğin menfaatine işlenmiş olmasıdır. Bu şart TCK'da "haksız menfaat sağlanan tüzel kişiler" demek suretiyle vurgulanmıştır. Sözleşme ayrıca suçun yönetici konumunda yer alan kişiler tarafından işlenmiş olması, şirketin yönetici konumunda olmayan çalışanların suçu işlemesi halinde ise şirketin bu çalışanı üzerinde denetim ve gözetim yükümlülüğünün ihlal edilmiş olması şartını da aramaktadır. AKSSS'nin (**Doğan,** s. 316).

olmaz ilkelerine aykırı olacaktır. Tüzel kişilerin nedensel değer taşıyan bir eylem gerçekleştirebilmesi ancak gerçek kişiler vasıtasıyla olabilmektedir.

Bu düzenleme karşısında tüzel kişi vasfına haiz servis sağlama hizmeti sunan şirketlerinde güvenlik tedbiri uygulaması şeklinde sorumluluğunun önü açılmış olacaktır. Ancak bunun için yukarıda sıralanan koşulların sağlanmış olması gerekmektedir[225].

Yaptırım konusunda son olarak belirtmeliyiz ki, TCK'nın 54 ve 55'nci maddelerinde belirtilen şartların bulunması halinde, eşya ve kazanç müsaderesi de söz konusu olabilecektir.

6. SORUŞTURMA USULÜ

TCK'nın 243'üncü maddesinde düzenlenen suçun takibi şikayete bağlı değildir, re'sen takibi gerekir. Zira bu maddede suçun şikayete tabi olarak kovuşturulacağına ilişkin bir kayıt bulunmamaktadır. Bununla birlikte, bu suçlarda mağdur ya da suçtan zarar görenlerin davaya katılma imkanı bulunmaktadır.

TCK'nın 243'üncü maddesinde yargılama yapmakla görevli mahkeme, maddede düzenlenen suç için öngörülen cezanın üst sınırı dikkate alındığında, 5235 sayılı Yasanın 10'uncu maddesi[226] uyarınca sulh ceza mahkemesidir.

SONUÇ VE DEĞERLENDİRME

Günümüzde bilişim teknolojilerinin hayatımızın her alanını kuşattığı, hatta yakın gelecekte bilişim olmaksızın hiçbir resmi (ve çoğu zaman özel) işlerimizi yürütemeyeceğimiz dikkate alındığında, bilişim sistemlerinin bilişim suçlularına karşı korunmasının mutlak bir zorunluluk olduğu görülecektir.

---

225 **Doğan,** s. 316.

226 Sulh ceza mahkemesinin görevi
Madde 10- Kanunların ayrıca görevli kıldığı haller saklı kalmak üzere, iki yıla kadar (iki yıl dahil) hapis cezaları ve bunlara bağlı adli para cezaları ile bağımsız olarak hükmedilecek adli para cezalarına ve güvenlik tedbirlerine ilişkin hükümlerin uygulanması, sulh ceza mahkemelerinin görevi içindedir.

Makalemizde de belirttiğimiz üzere bilişim suçlarının işlenebilmesi için öncelikle bilişim sistemine girmek gerektiğinden yetkisiz girişlerin suç olarak düzenlenmesi gerekmektedir. Bu nedenle TCK'nın 243'ncü maddesindeki düzenlemenin son derece yerinde bir düzenleme olduğunu düşünüyoruz. Ancak kanaatimizce aşağıda belirtilen hususların da yerine getirilmesi gerekmektedir.

- TCK'nın 243 (2)'nci maddesinde düzenlenen indirim sebebine ilişkin düzenlemenin hukuka aykırı giriş suçunun düzenleniş amacına göre, TCK'nın 163 (1) maddesindeki hüküm de göz önünde bulundurularak, tekrar ele alınması gerekir.

- TCK'nın 244'ncü maddesinde düzenlenen ancak 243'ncü maddede yer verilmeyen "sisteme girip kalma" fiilinin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali 243'ncü madde için de cezayı artıran hal olarak düzenlenmelidir.

- Bu suçun kamu görevlileri tarafından görevin sağladığı kolaylığın kötüye kullanılması suretiyle işlenmesi hali cezayı artıran hal olarak düzenlenmelidir.

- TCK'nın 243 ve 244'üncü maddeleri tek bir maddede birleştirilmeli ve 243 (1) maddesi suçun temel şekli olarak düzenlenerek diğer haller suçun nitelikli haline dönüştürülmelidir. Ancak bu yasal düzenleme yapılırken kişilerin özel hayatların gizliliğine ve mahremiyet haklarına mümkün olan en az müdahalede bulunulmalıdır. Ayrıca kanuni düzenlemeler yapılırken gelişen teknoloji ile birlikte mevzuat da sürekli takip edilip ikisi arasında eşgüdüm sağlanmalıdır. Mevzuat ve teknoloji birbirine paralel olarak ilerlemeli, mevzuatın teknolojinin gerisinde kalmasına engel olunmalıdır.

- Bilişimin toplum hayatındaki önemi dikkate alınarak cezalar yükseltilmelidir.

- TCK'nın 243'üncü maddesinde belirtilen suçların taksirle işlenmesi hali de cezalandırılmalıdır. Zira, bilişim artık hayatımızı tamamen kuşatmıştır ve bu suçların taksirli halleri de çok ciddi zararlar verebilmektedir.

- Bir sisteme rızayla girildikten sonra sistem sahibinin rızasının kalkması halinde girişte rıza bulunduğu için sisteme girme ve kalma suçu oluşmayacağını kabul ettiğimizden, tıpkı konut dokunulmazlığını ihlal suçunda olduğu gibi rızanın kalkması halinde failin sistemden çıkmaması durumu da suç olarak düzenlenmelidir.

- Bilişim alanında delil toplamanın güçlüğü dikkate alınarak adli bilişim bir bilim dalı olarak kabul edilmeli ve adli tıp benzeri bir yapılanma kurularak bu birimin ülke çapında teşkilatlanması sağlanmalıdır. Bu noktada belirtmeliyiz ki, bunun sıra yargı teşkilatının ve kolluk kuvvetlerinin sürekli eğitimi sağlanmalı ve bu kişilerin hukuki ve teknik bilgileri güncel tutulmalıdır.

- Bilişim alanında coğrafi sınırlar bulunmadığından, bilişim suçları ile mücadelede ulusal tedbirler yetersiz kalmaktadır. Bilişim suçları konusunda, mutlaka uluslararası işbirliğine gidilmeli ve imzaladığımız ancak uygun bulma kanununu henüz çıkarmadığımız AKSSS'nin uygun bulunmasına dair kanun biran evvel çıkarılmalıdır. Ayrıca AKSSS'nin 6'ncı maddesi gereğince, sözleşmenin 2-5'nci maddeleri arasında belirtilen suçları işlemek niyetiyle bir bilgisayar sisteminin tamamına veya bir bölümüne erişebilmek için bir bilgisayar şifresinin, erişim kodunun veya benzeri bir datanın üretimi, satışı, kullanım için elde edilmesi, ithali, dağıtımı veya temin edilmesi veya sahip olunması suç olarak düzenlenmelidir.

Kaynakça

KİTAPLAR

Artuk Mehmet Emin/**Gökçen** Ahmet/**Yenidünya** Ahmet Caner, Türk Ceza Kanunu Şerhi, 5. Cilt, Ankara, Turhan Kitapevi, 2009.

Artuk Mehmet Emin/**Gökçen** Ahmet/**Yenidünya** Ahmet Caner, Ceza Hukuku Özel Hükümler, 9.Basım, Ankara, Turhan Kitapevi, 2008.

Artuk Mehmet Emin/**Gökçen** Ahmet/**Yenidünya** Ahmet Caner, Ceza Hukuku Genel Hükümler, 3 Basım, Ankara, Turhan Kitapevi, 2007.

Avrupa Komisyonu Siber Suç Sözleşmesi Metni, tercüme edip aktaran Ankara Barosu Siber Suç Uzmanları Komitesi, 3. Basım Ankara Barosu Yayını, Ankara 2008.

Avşar B.Zakir/**Öngören** Gürsel, Bilişim Hukuku, İstanbul, Türkiye Bankalar Birliği Yayınları, Yayın No:270, 2010.

Aydın Emin Doğan, Bilişim Suçları ve Hukukuna Giriş, Ankara, Doruk Yayınları, 1992.

Aydın Nurullah, Türk Suç ve Ceza Hukuku Genel ve Özel Hükümler,2. Basım, Ankara, Adalet Yayınevi, 2009.

Centel Nur/**Zafer** Hamide, Ceza Muhakemesi Hukuku, 5.Basım, İstanbul, Beta Yayınevi, 2008.

Centel Nur/**Zafer** Hamide/**Çakmut** Özlem, Türk Ceza Hukukuna Giriş, İstanbul, BetaYayınevi, 2005.

Çekiç Burak, İnternet Aracılığıyla İşlenen Suçlar, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Anabilim Dalı, Kamu Hukuku Bilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2006.

Demircan Tunç, Bilişim Alanında Suçlar, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yayınlanmamış Yüksek Lisans Tezi, Konya, 2007.

Dülger Murat Volkan, Bilişim Suçları, Ankara, Seçkin Yayınevi, 2004.

Ergün İsmail, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara, Adalet Yayınevi, 2008.

Esen Sinan, Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanındaki Suçlar, Ankara, Adalet Yayınevi, 2007.

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

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

Kızıltan Mehmet Burak, "5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları", İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, yayınlanmamış yüksek lisans tezi, 2007.

Kiremitçioğlu Ali/**Tekin** Taylan, "Bilişim Suçları ve Etkin Mücadele Yöntemleri", 14-15 Mayıs 2005 Polis Bilişim Sempozyumu, Emniyet Genel Müdürlüğü Yayını, Kataloğ No:395.

Koca Mahmut/**Üzülmez** İlhan, Türk Ceza Hukuku Genel Hükümler, Ankara, Seçkin Yayınevi, 2008.

Köksal Aydın, Adı Bilgisayar Olsun, Cumhuriyet Kitapları, Bilişim Yazıları, Ankara, 2010.

Köksal Aydın, Bilişim Terimleri Sözlüğü, Türk Dil Kurumu Yayınları, Ankara Üniversitesi Basımevi, Ankara, 1991.

Kunter Nurullah/**Yenisey** Feridun/**Nuhoğlu** Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 17.Basım, İstanbul, Beta Yayınevi, 2009.

Kurt Levent, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları, Ankara, Seçkin Yayınevi, 2005.

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

Meran Necati, Yeni Türk Ceza Kanununda Sahtecilik - Malvarlığı - Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Ankara, Seçkin Yayınevi, 2005.

Öngören Gürsel, İnternet Hukuku, İstanbul, Öngören Hukuk Yayınları, Yayın No:1.2006.

Özbek Veli Özer/**Kanbur** Nihat/**Doğan** Koray/**Bacaksız** Pınar/**Tepe** İlker, Türk Ceza Hukuku Özel Hükümler, Ankara, Seçkin Yayıncılık, 2010.

Özgenç İzzet, Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), Ankara Açık Ceza İnfaz Kurumu Matbaası, 3.Basım, 2006.

Pallı Hayati, Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Kayseri, 2008.

Parlar Ali, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara, 2011.

Soyaslan Doğan, Ceza Hukuku Özel Hükümler, 8.Basım, Yetkin Yayınevi, Ankara, 2010.

Taşdemir Kubilay, Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara, Cantekin Matbaacılık, 2009.

Taşkın Şaban Cankat, Bilişim Suçları, İstanbul, Beta Yayınevi, 2008.

Ünver Yener/**Hakeri** Hakan, Ceza Muhakemesi Hukuku, 3.Basım, Ankara, Adalet yayınevi, 2010.

Yaşar Osman/**Gökçan** Hasan Tahsin/**Artuç** Mustafa, Yorumlu, Uygulamalı Türk Ceza Kanunu, Cilt:5, Ankara, Adalet Yayınevi, 2010.

Yaycı Esra, "Bilişim Suçları" Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Ceza ve Usul Hukuku Bilim Dalı, yayınlanmamış yüksek lisans tezi, Ankara, 2007.

Yazıcıoğlu Recep Yılmaz, Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile, İstanbul, Alfa Yayınevi, 1997.

DERGİLER ve ARMAĞANLAR

Akıncı Füsun **Sokullu**, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi" İnternet Özel Bölümü, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı:1-2, İstanbul, 2001.

Akıncı Hatice/**Alıç** A.Emre/**Er** Cüneyd, "TCK ve Bilişim Suçları", İnternet ve Hukuk (Derleyen Yeşim M. A. **Tamer**), İst. Bilgi Ünv. Yayınları,

Biçkin İnci, "Siber Suç Sözleşmesi ve 5237 s. Türk Ceza Kanununda Bilişim Suçları", Yargıtay Dergisi, Cilt:32, Ocak-Nisan 2006, Sayı:1-2.

Çankaya Ayhan, "Bilişim Suçlarıyla Mücadelede Gelinen Durum", Bilişim Hukuku, İstanbul, Kadir Has Üniversitesi Yayınları, Derleyen Mete **Tevetoğlu**, 2006.

Çeken Hüseyin, "Amerika Birleşik Devletlerinde İnternet Yolu İle İşlenen Suçlara İlişkin Düzenlemeler", Ankara, Askeri Adalet Dergisi, Sayı 144, Mayıs 2002.

Dalkılıç Aysun, "Avrupa Birliğine Uyum Sürecinde Bilişim Suçları", Avrupa Birliğine Uyum Sürecinde Türk Ceza ve Ceza Muhakemesi Hukuku, Proje Yöneticisi Prof.Dr. Fatih Selami **Mahmutoğlu**, İstabul Barosu Yayınları, İstanbul, 2008.

Değirmenci Olgun, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", Türkiye Barolar Birliği Dergisi, Yıl:18, sayı58, Mayıs-Haziran 2005.

Doğan Koray, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", Hukuk ve Adalet Eleştirel Hukuk Dergisi Yıl:2 Sayı 6-7, Ekim 2005.

Dülger Murat Volkan, "Yeni Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları ve Bu Suçlarla Mücadelede Alınması Gereken Önlemler" 14-15 Mayıs 2005 Polis Bilişim Sempozyumu, Emniyet Genel Müdürlüğü Yayını, Kataloğ No:395.

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:19, Sayı: 62, Ocak-Şubat 2006.

Er Cüneyd, "Bilişim Suçları", Bilişim Teknolojisi Hukuku Gündemi, 2003-2004, İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi Yayını, 2004.

Erdoğan Yavuz, "Gönüllü Vazgeçme", Ceza Hukuku Dergisi, Yıl:5, Sayı:13, Ağustos 2010.

Ersoy Yüksel, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", Prof.Dr Yılmaz GÜNAL'a Armağan, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, Cilt:49, No:3-4, 1994.

Flanagan Anne, "The Law and Computer Crime: Reading the Script of Reform", İnternational Journal of Law and Information Technology, Vol:13, No:1, Oxford University Press, 2005.

Gülşen Recep, "İnternet ve Suç", İnternet ve Toplum, Editör, Ahmet **Tarcan**, Ankara, Anı Yayıncılık, 2005.

Kadir Rizgar Mohammed, "The Scope and the Nature of Computer Crimes Statutes A Critical Comparative Study", German Law Journal, June, 2010.

Kiremitçioğlu Ali/**Tekin** Taylan, "Bilişim Suçları ve Etkin Mücadele Yöntemleri", 14-15 Mayıs 2005 Polis Bilişim Sempozyumu, Emniyet Genel Müdürlüğü Yayını, Kataloğ No:395, 2005.

Koca Mahmut, "Hukukumuzda TCK'nın 244 ncü maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı, Ankara, Yargıtay Başkanlığı Yayını, 2009.

Schjolberg Stein/**Hubbard** Amanda M., "Harmonizing National Legal Approaches on Cybercrime", International Telecommunication Union WSIS Thematic Meeting on Cybercrime Geneva 28 June- 1 July 2005.

Taşkın Şaban Cankat, "Bilişim Hukuku Uluslararası Uyuşmazlıklar", Türkiye Barolar Birliği Dergisi, sayı:85, Aralık 2009.

Tepe İlker, "İnternet (Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukuku'ndaki Yeni Gelişmeler" Alman Türk Karşılaştırmalı Ceza Hukuku, Yayına Hazırlayanlar Prof Dr Dr. Eric **Hilgendorf**, Prof Dr Yener **Ünver**, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi Yayın No:17, 2010.

Ünver Yener, "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası İnternet özel Bölümü, Cilt:LIX, Sayı:1-2, 2001.

Valerius Brian, "Almanya'da İnternet Ceza Hukuku" Alman Türk Karşılaştırmalı Ceza Hukuku, Çeviren Rabia ÜNLÜ, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi Yayınları, Yayın no:17, 2010.

Yazıcıoğlu Recep Yılmaz, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını, Ankara 2009.

Yazıcıoğlu Recep Yılmaz, "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi" Hukuk ve Adalet Eleştirel Hukuk Dergisi, Yıl:1, Sayı:1, Ocak-Mart 2004.

Yazıcıoğlu Recep Yılmaz, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt:II, Sayı:2 Yıl 2005

Yenidünya Ahmet Caner, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu ", Legal Fikri ve Sınai Haklar Dergisi, İstanbul, Aralık2005, Sayı:4.

Yılmaz Sacit, "5237 Sayılı TCK'nın 244.Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", Türkiye Barolar Birliği Dergisi, 2011 (92).

İNTERNET

Avar Elif, "Bilgisayar Suçları ve Virüsler", http://arsiv.aksiyon.com.tr/arsiv/233/pages/dosyalar/dos1.html, 21.01.2010.

Mariana Sandra, Cyber Crime: a Comparative Law Analysis, http://uir.unisa.ac.za/bitstream/10500/2056/17/03chapter3.pdf 21.07.2010.

Schjolberg Stein, www.mossbyrett.of.no/info/legal.html, 19.12.2005, Aktaran, **Artuk** Mehmet Emin/**Gökçen** Ahmet/**Yenidünya** Ahmet Caner, Türk Ceza Kanunu Şerhi, 5. Cilt, Ankara, Turhan Kitapevi, 2009.

http://tdkterim.gov.tr 18.03.2010.

http://tr.wikipedia.org/wiki/Bluetooth, 19.03.2010.

http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.sorgu_yonlendirme, 08.04.2011

http://www.wifi-turk.com/makale-8-wi-fi-nedir-ve-bluetooth-arasindaki-farklar.html, 19.03.2010.