[H] BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME VEYA BOZMA SUÇU VE UYGULAMADAKİ SALDIRI TÜRLERİ

(THE CRIME OF HINDRANCE OR DESTRUCTION OF THE INFORMATION SYSTEM AND TYPES OF ATTACKS IN PRACTICE)

Dr. Gürkan ÖZOCAK [*] [**]

ÖZET

Bilişim suçları Türk Ceza Kanunu'nun (TCK) 243 ilâ 246. maddelerinde düzenlenmiş olup, bu suçların en önemlilerinden biri TCK'nın 244/1. maddesinde öngörülen bilişim sisteminin işleyişini engelleme veya bozma suçudur. Bu suç, bilişim (IT) sisteminin çeşitli teknik yöntemlerle geçici olarak durdurulması veya işlevini yerine getiremeyecek hale sokulması yollarıyla işlenebilmektedir. Uygulamada bu suçun en sık görülen türleri arasında DoS ve DDoS saldırıları, Tavşan (Rabbits) saldırıları ve SPAM'ler sayılabilir.

ANAHTAR SÖZCÜKLER

Bilişim suçları, bilişim sisteminin işleyişinin engellenmesi veya bozulması, siber saldırı, DDoS.

SUMMARY

Cybercrimes are regulated in articles 243 to 246 of the Turkish Penal Code (TPC) and one of the vital types of these crimes is the hindrance or destruction of the information system which is regulated in Article 244/1 of TPC. The crime can be committed by temporarily hindrance the information (IT) system or rendering it inoperable by various technical methods. The most common types of this crime in practice include DoS and DDoS attacks, Rabbits attacks and SPAMs.

[H] Eserin Dergimize geliş tarihi: 05.11.2023. İlk hakem raporu tarihi: 28.12.2023. İkinci hakem raporu tarihi: 17.01.2024. Onaylanma Tarihi: 17.01.2024.

[*] Doktor, İstanbul Gedik Üniversitesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

[**] Yazarın ORCID belirleyicisi: 0000-0002-5098-7697.

Esere Atıf Şekli: Gürkan Özocak, "*Bilişim Sisteminin İşleyişini Engelleme veya Bozma Suçu ve Uygulamadaki Saldırı Türleri*", YÜHFD, C.XXI, 2024/1, s. 257-291.

KEYWORDS

Cyber crimes, hindrance or destruction of the information system, cyber-attack, DDoS.

I. GİRİŞ

Son yıllarda teknolojinin gelişmesiyle birlikte, işlenen suç tipleri de değişmekte ve bilişim yoluyla işlenen suçların sayısı günden güne artmaktadır. Bilişim ve özellikle bilgisayar sistemlerinin yaygınlaşması ile beraber ceza hukuku alanında, bu sistemlerin kötüye kullanımlarına ilişkin fiillerin cezalandırılabilirliği konusu gündeme gelmiş ve son dönem ceza kanunlarının hepsinde "*bilgisayar suçları*", "*bilişim suçları*" veya "*siber suçlar*" olarak adlandırılan suç tipleri düzenlenmeye başlanmıştır[1].

Bu husus 2004 tarihinde yürürlüğe giren ve Kasım 2010 itibariyle Türkiye'nin de tarafı haline geldiği Avrupa Konseyi Siber Suç Sözleşmesi'nde de düzenlenmiş olup, Sözleşmenin 4, 5 ve 6. maddelerinde, "*Veriye Müdahale*", "*Sisteme Müdahale*" ve "*Cihazların Kötüye Kötüye Kullanılması*" eylemlerinin, Sözleşme tarafı ülkelerin ulusal kanunlarında suç olarak düzenlenmesi gerektiği ifade edilmiştir[2]. Bu bağlamda, Sözleşme yürürlüğe girdikten sonra ve fakat Türkiye Sözleşmeye taraf olmadan önce yürürlüğe giren 1 Haziran 2005 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda da, 243 ilâ 246. maddeler arasında "*Bilişim Alanında Suçlar*" başlığı altında, Siber Suç Sözleşmesi'nde de öngörülen bu eylemler suç olarak düzenlenmiştir.

Buna göre, 'Bilişim Alanında Suçlar' başlığı altında, TCK m. 243/1'de bilişim sistemlerine hukuka aykırı olarak girme (yetkisiz erişim), TCK m. 243/4'de bilişim sistemindeki veri nakillerini sisteme girmeksizin teknik araçlarla izleme, TCK m. 244/1'de bir bilişim sisteminin işleyişinin

[1] **Köksal Bayraktar/Zeynel T. Kangal/Ali Hakan Evik/Pınar Memiş Kartal/Fulya Eroğlu/Vesile Sonay Evik/Ali Kemal Yıldız/Eylem Aksoy Retornaz/Gülşah Bostancı Bozbayındır/Asuman Aytekin İnceoğlu**, Özel Ceza Hukuku, Ekonomi, Sanayi ve Ticarete İlişkin Suçlar – Bilişim Alanında Suçlar, Cilt VIII, İstanbul, 2021, s. 220 (Bayraktar ve diğerleri); **Muammer Ketizmen**, Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008, s. 32.

[2] Avrupa Konseyi Siber Suç Sözleşmesi'nin hazırlanma süreci ile düzenlediği maddi ceza hukuku ve ceza muhakemesi hukuku kuralları hakkında detaylı bilgi ve değerlendirme için bkz. **Ulrich Sieber**, "*Bilgi Toplumunda Ceza Hukuku ve Dijitalleşme – Bilişim Suçları*", Çeviren: Prof. Dr. Feridun Yenisey – Av. Damla Zaimoğlu, Bilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku, Ankara, 2021, s. 265 vd.

engellenmesi veya bozulması, TCK m. 244/2'de bir bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi ve var olan verilerin başka yere gönderilmesi, TCK m. 245'te banka ve kredi kartı üzerinde işlenen fiiller ve nihayet TCK m. 245/A'da bilişim suçlarının işlenmesi için üretilen yasak cihaz veya programlar üzerinde işlenen fiiller suç olarak öngörülmüştür[3].

Çalışmamızın konusunu TCK m. 244/1'de düzenlenen "*Bilişim Sisteminin İşleyişini Engelleme veya Bozma Suçu*" oluşturmaktadır. Esasen TCK m. 244'ün genel ve soyut tanımını verdiği suç tipleri "*seçimlik hareketli suçlar*"dan[4] olup, buna karşın teknolojinin ilerlemesiyle doğru orantılı olarak, bu suçların işlenmesinin sayısız yöntemi de ortaya çıkmıştır. Bununla beraber, hükmün birinci ve ikinci fıkralarında birbirlerinden farklı suç tipleri düzenlenmektedir. Birinci fıkrada doğrudan bilişim sistemi üzerinde işlenen fiiller suç olarak öngörülmüşken, ikinci fıkrada ise sistemin içerisindeki verilere yönelik çeşitli fiiller seçimlik hareketli suç kapsamında düzenleme alanı bulmuştur. Çalışmamızda, yalnızca birinci fıkrada düzenlenen bilişim sisteminin işleyişinin engellenmesi veya bozulması fiilleri ile bu suç tipinin uygulamada sık görülen örnekleri üzerinde durulacaktır.

II. BİLİŞİM ALANINDA SUÇLAR

A) BİLİŞİM SUÇU KAVRAMI

Doktrinde kimi zaman birbirinin yerine de sıkça kullanılan *"bilişim suçları"* veya *"bilgisayar suçları"* ile ilgili ortak bir tanımlama yapılamamış, birçok yazar bu suçlara kendince bir sınır çizmiştir[5]. Çalışmamızın kapsamı bakımından bu tartışmaların tamamını buraya alamamakla birlikte[6], son

[3] Mülga 765 sy. TCK'ndaki bilişim alanında suçlar düzenlemesi ve sistematiği hakkında detaylı bilgi için Bkz. **Ketizmen**, s. 58 vd.; **Murat Volkan Dülger,** Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, 2014, s. 219-310.

[4]**Olgun Değirmenci,** "*2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi*", Türkiye Barolar Birliği Dergisi, Sayı: 58, Ankara, 2005, s. 205.
Ayrıca seçimlik hareketli suçlarla ilgili Bkz. **Sulhi Dönmezer/Sahir Erman**, Nazari ve Tatbiki Ceza Hukuku, Cilt: I, İstanbul, 1987, s. 361 **(C. I)**; **Nevzat Toroslu/Haluk Toroslu**, Ceza Hukuku Genel Kısım, Ankara, 2019, s. 138 vd.

[5] **Berrin Bozdoğan Akbulut**, "*Bilişim Suçları*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, Sayı: 1-2, Cilt: 8, Konya, 2000, s. 550.

[6] Tartışmalar için Bkz. Bayraktar ve diğerleri, s. 221 vd.; **Mehmet Can Karagöz**, Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, İstanbul, 2020, s. 83 vd.; **Ketizmen**, s. 32-54; **Levent Kurt**, Tüm

tahlilde bilişim suçları, verilerin bilişim temelli olarak ve otomatik bir biçimde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içerisinde işlenen, bir bilgisayara veya bilgisayar ağına yahut bir bilişim sisteminin bir kısmına ya da tamamına yönelik olarak veya onları araç olarak kullanarak icra edilen ve ceza normunda suç olarak düzenlenmiş fiiller olarak tanımlanabilir[7].

Bilişim suçlarını "*bilişim sistemleri aracılığıyla işlenen suçlar*" ve "*bilişim alanındaki suçlar*" olarak ikiye ayırmamız mümkündür. İlk gruptaki suçlar "*geleneksel*" ya da "*klasik*" suçlar olarak adlandırılabilecek, yani bilişim sistemi haricinde yollarla da işlenebilen, ancak somut olayda bir bilişim sistemi aracılığıyla işlenmiş suçlardır. Örneğin; e-posta yoluyla veya sosyal medya kanalları üzerinden işlenen tehdit veya hakaret suçu, yine bilgisayar veya İnternet siteleri üzerinden işlenen cinsel taciz, halkı kin ve düşmanlığa tahrik etme gibi suçlar bu grupta sayılabilir. Yukarıda sayılan suçlar farklı yöntemlerle de işlenebilirlerse de, bilişim sistemleri araç olarak kullanılarak işlenmeleri halinde bilişim suçlarının inceleme alanına girmektedirler. Teknolojik olanakların müthiş bir hızla artması ve gelişmesi, buna bağlı olarak da siber suçluluğun sınırlarının ciddi bir şekilde genişlemesi ile birlikte, günümüzde kasten insan öldürme suçuna kadar hemen her suç tipi bilişim yoluyla işlenebileceği için, bu gruptaki suçların sınırını çizmek veya bunları tasniflemek mümkün değildir[8].

İkinci gruptaki suçlar ise, TCK'da sınırlı sayıda düzenlenen ve ilk gruptaki suçlara göre teknik özellikler arzeden, başka bir deyişle davranış ve sonuç aşamalarının tamamı kural olarak bilişim alanında gerçekleşip sona eren suçlardır. 5237 sy. TCK'da bu suçlar, 243 ila 246. maddeler arasında, "*Bilişim Alanında Suçlar*" başlığıyla düzenlenmiştir[9].

Çalışmamızın konusunu oluşturan, "*bilişim sisteminin işleyişini bozma veya engelleme suçu*" da bu ikinci grupta incelenmesi gereken, TCK m. 244/1'de düzenlenen ve işlenişi bakımından ilk gruptaki suçlardan farklı özellik arzeden bir bilişim suçudur.

Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005, s. 49-53; **Hasan Sınar**, İnternet ve Ceza Hukuku, İstanbul, 2001, s. 69-78.

[7] **Kurt**, s. 53; **Muharrem Özen/İhsan Baştürk**, Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011, s. 90-91.

[8] **Ali Osman Özdilek**, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul, 2006, s. 112.

[9] Bunlara, kanun tarafından sınırlı sayıda öngörüldükleri için "*dar anlamda bilişim suçları*" da denilmektedir. Bkz. **Özen/Baştürk**, s. 113.

B) GENEL OLARAK BİLİŞİM ALANINDA SUÇLAR ve 5237 SAYILI TÜRK CEZA KANUNU'NUN SİSTEMİ

Bilişim alanında suçlar, Mülga 765 sayılı TCK'da "*mal aleyhine cürümler*" kapsamında değerlendirilmiş ve ayrı bir bapta düzenlenmiş olup[10], 5237 sayılı TCK ile "*Bilişim Alanında Suçlar*" başlığıyla, Kanunun Üçüncü Kısmı olan "*Topluma Karşı Suçlar*" arasında düzenlenmiştir. 765 sayılı TCK'da, özel kısmın sistematiği olan hukuki konu esasından vazgeçilerek bu suçların ayrı bir bab altında düzenlenmesi, söz konusu düzenlemeyi yapan 1991 tarihli 3765 sayılı değişiklik kanunun gerekçesinde şu şekilde açıklanmıştır: "*Yabancı kanunlardan bir kısmı, bilişim alanındaki suçları ayrı bir bölümde toplayarak ilgili suç bölümlerine yerleştirmektedirler. Kanunda ise bu suçların uygulamada kolaylık sağlamak üzere ayrı bir bölümde düzenlenmesi tercih edilmiştir*."[11]

5237 sayılı TCK'da ise, Alman ve İtalyan ceza kanunlarında hâkim olan anlayış kabul edilerek, "*Bilişim Alanında Suçlar*" üçüncü kısmın onuncu bölümünde "*Topluma Karşı Suçlar*" ana başlığı altında düzenlenmiş ve yapılan tasnifte, ceza kanununda esas alınan hukuki konu ölçütü nazara alınmıştır[12].

İtalyan Ceza Kanunu'na ("*İCK*") bakıldığında, bilişim alanında suçların hukuki konularına göre tasnif edildiği ve farklı başlıklarda düzenlendiği görülmektedir. Örneğin, TCK m. 243'te düzenlenen "*bilişim sistemine girme (yetkisiz erişim)*" suçu, İCK m. 615 ter'de "*Özel Hayata Hukuka Aykırı Müdahale*" (*Interferenze illecite nella vita private*) hükmünden hemen sonra düzenlenmekte ve başkasının "*enformatik veya telematik*" sistemine giren

---

[10] **Özen/Baştürk**, s. 111.

Ayrıca düzenleme ve nedenleri hakkında bkz. **Kubilay Taşdemir/ Ramazan Özkepir**, Mala Karşı Suçlar, Ankara, 1993, s. 507.

Değişikliğin yapıldığı dönemde, bilgisayarın giderek gündelik yaşamın bir parçası durumuna geldiği ve bu nedenle yeni suç türleri ortaya çıktığı, özellikle özel kuruluşların bilgisayar sistemlerine girilerek bu kuruluşların ticari bilgilerinin elde edilmesi ve kullanılması gibi durumlar söz konusu olduğundan, TCK'da bilişim suçları konusunda yasal bir düzenleme yapılması gerekliliğinin ortaya çıktığı söylenmiştir. Bkz. **Faruk Erem**, "*Bilgisayar Suçları ve TCY*", Yargıtay Dergisi, Cilt: 17, Sayı: 4, Ekim 1991, s. 436-437.

[11] **TBMM Tutanak Dergisi**, 6.6.1991, Dönem 18, Yıl 4, C. 61, Birleşim 119-131, s. 17, Sayfa Sayısı 513, Aktaran **Yılmaz Yazıcıoğlu**, Kriminolojik, Sosyolojik ve Hukuki Boyutları İle Bilgisayar Suçları, İstanbul, 1997, s. 212.

[12] **Ketizmen**, s. 60.

kimsenin üç yıla kadar hapis cezasıyla cezalandırılacağı öngörmektedir[13]. Buna karşın, çalışmamızın da konusunu oluşturan "*sisteme veya veriye müdahale*" fiili, İCK'nin malvarlığı aleyhine suçlar kısmında, "*Mala Zarar Verme*" (*Danneggiamento*) suçundan hemen sonra gelmek üzere, 635 bis maddesinde düzenlenmektedir. Bu hükme göre ise, enformatik ve telematik sistemlerin, programların, verilere zarar verilmesi, bozulması, tamamen ya da kısmen kullanılamaz hale gelmesi halinde fail cezalandırılmaktadır[14].

Alman Ceza Kanunu'nda da mala zarar verme suçunda eşyaya maddi etkide bulunulmasının yeterli olduğu, örneğin işlem kabiliyetinin bozulmasının bu suçun varlığına yeteceği, bunun dışında fiziki yapısının bozulmasının gerekmediği anlayışı kabul edilerek, sisteme ve veriye müdahale suçu malvarlığına karşı suçlar arasında sayılmaktadır[15].

Bu anlayışla yapılan düzenleme sonucu, "*Bilişim Alanında Suçlar"* 5237 sy. Kanun'un 243, 244, 245 ve 245/A maddelerinde düzenlenmiştir. Ne var ki, hukuki konu ölçütüne göre tasnifte Alman ve İtalyan ceza kanunlarını nazara alan kanun koyucu, bu suçları "*Topluma Karşı Suçlar*" arasında düzenlemiştir. Bu suçların hukuki konusuyla ilgili tartışmaya aşağıda ayrıca değinilecektir. Ancak bu kategorik tartışmalardan bağımsız olarak bahsi geçen suçları tasnif edecek olursak, TCK, "*Bilişim Alanında Suçlar*"ı şu suçlar olarak sınırlandırmaktadır: "*Bilişim Sistemine Girme* (*Yetkisiz Erişim)", "Bilişim Sisteminin İşleyişini Engelleme ve Bozma", "Bilişim Sistemindeki Verilere Müdahale (Verileri Bozma, Yok Etme, Değiştirme, Erişilmez Kılma, Sisteme Veri Yerleştirme ve Var Olan Verileri Başka Bir Yere Gönderme)", "Bilişim Sistemleri Aracılığıyla Yarar Sağlama", "Veri Nakillerini Sisteme Girmeksizin Teknik Araçlarla İzleme", "Yasak Cihaz ve*

[13] "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni."İCK'da bilgisayar veya bilişim yerine, bilişim alanındaki suçlarla ilgili "enformatik veya telematik" (informatico o telematico) terimleri kullanılmaktadır. "Enformatik terimi, enformasyon kelimesinin otomatik kelimesiyle birleşmesinden ortaya çıkmaktadır. Bu haliyle, elektronik hesaplama makineleri yardımıyla enformasyonun otomatik olarak temsil edilmesi, iletilmesi, dönüştürülmesi ve hesaplanmasını ifade etmektedir. Enformatik araçlarının iletişim kurarak birbirine bağlanması ise, telematik terimini ortaya çıkarmaktadır. Her iki terimin bir araya gelmesi ise 'telekomünikasyon ve enformatik' terimini ortaya çıkarmaktadır" Bkz. **Salvatore Resta**, Computer Crimes Tra Informatica e Telematica, Cedam, 2000, s. 7.

[14] "Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni."

[15] **Hans-Heinrich Jescheck**, Alman Ceza Hukukuna Giriş, Çev. Feridun Yenisey, İstanbul, 2007, s. 108-109.

Programlar Üzerinde İşlenen Fiiller" ve *"Banka ve Kredi Kartlarının Kötüye Kullanımı*".

III. BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİN ENGELLENMESİ VEYA BOZULMASI SUÇU

A) GENEL OLARAK

TCK'nın 244. maddesinin birinci fıkrasında "*bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."* denilmekte, ikinci fıkrasında ise "*bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır"* hükmüyle sistemdeki veriler üzerinde işlenen bazı fiiller suç olarak düzenlenmektedir.

Yasal düzenlemeden görüleceği üzere, TCK m. 244 "*sisteme ve veriye müdahale*" şapkası altında, birçok fiili suç kapsamına almaktadır. Bu bağlamda, failin bir bilişim sisteminin işleyişini engellemesi veya bozması (sisteme müdahale), bununla beraber bilişim sisteminin içerisindeki verileri bozması, yok etmesi, değiştirmesi, erişilmez kılması, bunun yanında sisteme veri yerleştirmesi yahut mevcut verileri başka bir yere göndererek sisteme zarar vermesi (veriye müdahale) ayrı ayrı suç sayılmaktadır.

Madde gerekçesine göre "*Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır*." Bu gerekçeden ve kanun koyucunun eğiliminden hareketle, öngörülen bu hükümle, günümüz dünyasında kişilerin hemen her işini yaptıkları bilgisayar ve bilişim sistemlerinin sağlıklı bir şekilde işlemesinin ve gerek bu sistemlerin gerekse de sistem içerisinde yer alan verilerin bütünlüğünün korunmasının amaçlandığı söylenebilir. Nitekim, kanunun yapıldığı dönemde, sosyo-ekonomik yapı içerisinde faaliyetlerin ağırlıklı olarak bilgisayar sistemleri aracılığıyla veri işleme şeklinde gerçekleştirilmeye başlanması ve günden güne bu işlemlerin yoğunlaşması, verilerin gizliliğine ve içeriğine ilişkin koruma yanında, mevcut verilerin varlığının, bütünlüğünün ve erişilebilirliğinin de korunmasını gündeme

getirmiştir[16]. Bu nedenle, kişisel verilerin korunmasına ilişkin mevzuatın yanında, özellikle bilişim sistemlerinin ve verilerin bütünlüğünün korunması amacıyla TCK m. 244 düzenlenmiştir.

Yukarıda ifade ettiğimiz üzere, TCK m. 244'te *"bilişim sistemi*" ve "*sistemin içerisindeki veriler*" olmak üzere iki ayrı koruma alanı söz konusudur. Bu koruma sisteminde Avrupa Konseyi Siber Suç Sözleşmesi'nin esas alındığını söylememiz doğru olacaktır. Zira, Siber Suç Sözleşmesi'nde de bilişim sistemine ve verilere müdahale hususu baz alınmış, veriye müdahale 4., sisteme müdahale ise 5. maddede düzenlenmiştir. Siber Suç Sözleşmesi'nin "Veriye Müdahale" *(Data interference)* başlıklı 4. maddesine göre "*Her bir taraf devlet, bir kimsenin bilgisayar verisine hakkı olmadığı halde, bilerek ve isteyerek zarar verme, silme, bozma, değiştirmeye ya da ortadan kaldırma fiilleri işlemesini suç olarak düzenlemek üzere gerekli kanuni düzenlemeyi yapmalı ve gerekli diğer önlemleri almalıdır*." Sözleşme'nin "Sisteme Müdahale" *(System interference)* başlıklı 5. maddesinde ise şu düzenleme yer almaktadır: "*Her bir taraf devlet veri yükleyerek, aktararak zarar vererek, silerek, bozarak, değiştirerek veya müdahale ederek bilgisayar sisteminin kullanımında hakkı olmadığı halde bilerek ve isteyerek bilgisayarın sisteminin çalışmasını sekteye uğratma fiilini ulusal kanununda suç olarak düzenlemeli ve gerekli diğer düzenlemeleri yapmalıdır.[17]"*

Sözleşmenin bilişim sistemine müdahale fiillerini düzenleyen 5. maddesine bakıldığında, suçun oluşumu için bilgisayar sisteminin fiziken zarar görmesinin aranmadığı, sistemin işleyişinin ciddi bir biçimde engellenmesinin veya bozulmasının yeterli olacağı, bu bağlamda da bilişim sisteminin maddi varlığını oluşturan donanımına yönelik fiziksel müdahalenin kapsam dışı bırakıldığı ifade edilmiştir[18]. Siber Suç Sözleşmesi'ndeki bu düzenleme ile ilgili tartışmalara ilerleyen bölümlerde ayrıca değinilecektir.

TCK m. 244'de de, Siber Suç Sözleşmesi'ne paralel bir biçimde, bilişim sistemine müdahale ile veriye müdahale fiilleri birbirinden ayrılmış ve hükmün birinci fıkrasında bilişim sistemine müdahale, ikinci fıkrasında ise sistem içerisindeki veriye müdahale fiilleri ayrı ayrı suç olarak düzenlemiştir.

Ceza hukuku mevzuatımızda bilişim sistemine ve veriye müdahaleye ilişkin ilk düzenleme, 3756 sy. Kanun ile 765 sy. TCK'ya eklenen 525/b

---

[16] **Ketizmen**, s. 112.
[17] Sözleşmenin maddi ceza hukukuna ilişkin düzenlemelerine ilişkin bkz. **Sieber**, s. 265-278.
[18] **Ketizmen**, s. 114-115.

maddesinin birinci fıkrasıdır. Bu ilk düzenlemeye göre, *"Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beşmilyon liradan ellimilyon liraya kadar ağır para cezası verilir." Dönmezer*'e göre, sisteme ve veriye müdahaleye dair yapılan bu düzenlemenin sebebi, bilgisayarın dokunulmaz olması gerekliliği ile beraber sistemin ve içeriğin de uygun bir şekilde işlev ve hizmet görmesidir. Bu şekilde, öncelikle malikin veya bilgisayar sistemini kullanan kişinin yararı korunmaktadır[19]. *Yazıcıoğlu*'na göre de, bu düzenleme ile kişilerin bilgisayar sistemleri ve içerikleri üzerindeki mülkiyet hakları korunmaktadır[20]. Bunun dışında, ayrıntılarda kimi farklılıklar olmakla beraber, Türk doktrinindeki yazarların büyük bir kısmı, 765 sy. Mülga TCK m. 525/b ile kişinin malvarlığının korunduğu hususunda mutabıktırlar[21].

2005 yılında yürürlüğe giren 5237 sy. TCK'nın 244. maddesi ile, 765 sy. TCK m. 525/b yürürlükten kalkmış ve sisteme ve veriye müdahale fiilleri, "Topluma Karşı Suçlar" ana başlığının altında, 244. maddede iki fıkra halinde düzenlenmiştir. Bu düzenleme, mülga kanunun aksine, 5237 sy. TCK bakımından sisteme ve veriye müdahale fiillerine ayrı ayrı ceza verileceği ve sisteme müdahalenin, veriye müdahaleye göre daha ağır bir cezayla karşı karşıya kalınacağı anlamı taşımaktadır.

B) SUÇUN HUKUKİ KONUSU

1. Genel Olarak Suçların Tasnifi ve Bilişim Sisteminin İşleyişini Engelleme veya Bozma Suçunun Hukuki Konusu

Suçlar, soyut ve akli bakımdan çok farklı şekillerde tasnif edilmiştir. Bu tasnif, manevi unsura, failin saikine, suçluya, failin sıfatına, pasif süjeye, verilecek cezaya, maddi konuya yahut hukuki konuya göre yapılabilmektedir. Hangi kriterin seçileceği, tasnifi yapan kimsenin güttüğü amaca göre

[19] **Sulhi Dönmezer**, Kişilere ve Mala Karşı Cürümler, İstanbul, 2001, s. 622.
[20] **Yazıcıoğlu**, s. 259.
[21] Bu görüşler ve farklılıklar için Bkz. **Ketizmen**, s. 117-118.

değişebilmektedir. Belirli bir amaç yönünden mükemmel görünen bir tasnif, farklı bir amaç esas alındığında yetersiz addedilebilir[22].

Çok uzun zamandır doktrinde hâkim olan görüş, özel kısmın sistematiğinin ve netice olarak da suçların tasnifinin, ancak özel suç tiplerinin hukuki konularının farklılığı kriterine istinaden inşa edilebileceği yönündedir. Gerçekten de bir ceza normunun anlamı ve kapsamının doğru bir şekilde tespiti, ancak hukuki konusunun, bir başka deyişle hangi menfaati koruma altına aldığının tespiti ile mümkündür[23]. Bu bakımdan, kanaatimizce de doğru olan, suçların tasnifinin hukuki konu ölçütüne göre yapılmasıdır.

Yukarıda bahsedildiği üzere, hukuki konu ölçütüne göre suç tasnifi yapan İtalyan Ceza Kanunu'nun 635 bis maddesinde malvarlığına karşı suçlar arasında, "Mala Zarar Verme" suçunun hemen sonrasında düzenlenen sisteme ve veriye müdahale suçları, Alman ve Fransız ceza kanunlarında da aynı şekilde hüküm altına alınmıştır. Bununla beraber, hukuki konu ölçütüne göre yapılan bu ayrım, klasik mala zarar verme suçlarıyla karşılaştırıldığında tartışmalara da yol açmaktadır[24].

Bu bakımdan değerlendirildiğinde, mala zarar verme suçu 5237 sy. TCK'nın 151. maddesinde düzenlenmekte olup, buna göre *"Başkasının taşınır veya taşınmaz malını kısmen veya tamamen yıkan, tahrip eden, yok eden, bozan, kullanılamaz hâle getiren veya kirleten kişi, mağdurun şikâyeti üzerine, dört aydan üç yıla kadar hapis veya adlî para cezası ile cezalandırılır."* Dolayısıyla, bir suçun mala zarar verme suçuyla aynı hukuki konuya sahip olduğu kanaatine varmak için, suçun üzerinde işlendiği maddi konusunun "*taşınır veya taşınmaz bir mal*" olduğunun tespiti gerekir. Donanım olarak bilgisayarın taşınır bir mal niteliğinde olduğuna şüphe yoktur. Esas tartışma, bilgisayarın verilerini de içerisinde bulunduran ve elle tutulur bir maddi varlığa sahip bulunmayan yazılım kısmıyla ilgilidir.

ABD'de, özellikle federe devletlerin ceza mevzuatlarında, ekonomik değeri olan veri de mal olarak kabul edilmekte ve veriye müdahale de malvarlığına karşı bir suç olarak düzenlenmektedir. İkinci bir yaklaşım ise, verinin somut bir varlığı olmadığından hareketle, veriyi mal olarak kabul etmemektedir. Bu yaklaşıma göre, verinin içerisinde saklandığı taşınır mal

[22] **Nevzat Toroslu**, Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Ankara, 1970, s. 45-47 **(Cürümlerin Tasnifi)**. Ayrıca suçların tasnifi bakımından uygulanan kriterlere ilişkin ayrıntılı bilgi için Bkz. **Toroslu**, Cürümlerin Tasnifi, s. 47-87.

[23] **Dönmezer/Erman**, C. I, s. 344 vd.; **Faruk Erem**, Ümanist Doktrin Açısından Türk Ceza Hukuku, C. I, Ankara, 1987, s. 248 vd.; **Toroslu**, Cürümlerin Tasnifi, s. 81-82.

[24] **Ketizmen**, s. 121.

(bilgisayar, bilgisayarın sabit diski vb.), taşıdığı veri ile birlikte bir işleve ve değere sahip olup, veriye veya sisteme müdahale sonucunda bu işleve zarar verildiğinden, bu şekilde mala zarar verme suçu oluşmaktadır[25].

Hangi yaklaşım kabul edilirse edilsin, çıkacak sonuç aynıdır. Bilişim sistemi ve bu sistemin yazılım unsuru veya içerisindeki veriler soyut varlıklarıyla bir mal niteliği taşımasalar da, bu soyut varlıklara müdahale edildiğinde, bunların saklandığı somut donanım da işlevini yitireceğinden, bir başka deyişle sisteminin işleyişi engellenmiş bir bilgisayarın veya içerisindeki verilere zarar verilmiş bir sabit diskin hiçbir değeri ve işlevi kalmayacağından, bu halde de mala zarar verme suçu meydana gelecektir. Bu itibarla, sisteme ve veriye müdahale suçları da, mala zarar verme suçu ile aynı hukuki konuya sahip suçlardır.

2. TCK m. 244'te Düzenlenen Suçun Hukuki Konusu

765 sy. TCK'nın yürürlükte olduğu dönemde, Kanunun 525/b maddesinde düzenlenen bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunun hukuki konusunun mala zarar verme suçu ile aynı olduğuna ilişkin, doktrinde neredeyse bir mutabakat bulunduğunu daha önce ifade etmiştik.

Ancak, bu hüküm 5237 sy. TCK'nın 244 maddesi ile ilga edilmiştir. Bazı yazarlarca, TCK m. 244 ile beraber bu suçların hukuki konularının değiştiği ve veri ve yazılımlardan oluşan soyut varlıkların yanında, somut nitelik arzeden donanım unsurunun da korunması nedeniyle, suçun hukuki konusunun karma nitelik gösterdiği söylenmiştir[26].

Bunun yanında bazı yazarlarca, düzenlenen bu suç ile öncelikle mülkiyet hakkının koruma altına alındığı savunulmaktadır. Zira hükmün koruma sağladığı alan, hem fizik, hem de soyut kavramları kapsamaktadır[27]. Öyle ki, kimi yazarlar bu görüşü daha da ileriye taşıyarak, TCK'nın 244. maddesi ile getirilen düzenlemenin, mala zarar verme suçunun özel bir şekli olduğunu ifade etmektedirler[28].

Kanaatimizce de, söz konusu suçların hukuki konusunun, 5237 sy. TCK'nda malvarlığına karşı suçlar kapsamından çıkarılarak "Topluma Karşı Suçlar" kısmının altında düzenlenseler ve soyut varlıklara müdahalenin söz konusu olması nedeniyle klasik mala zarar verme suçlarıyla birebir

[25] **Ketizmen**, s. 123-124.
[26] **Murat Volkan Dülger**, Bilişim Suçları, Ankara, 2004, s. 231.
[27] **Kurt**, s. 161-162.
[28] **Ali Karagülmez**, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara, 2005, s. 187.

örtüşmeseler de, veri ve programlara müdahale durumunda, bunları içeren donanımın da işlevini kaybedecek olması nedeniyle, mala zarar vermenin hukuki konusuyla paralellik taşıdığını kabul etmek gerekmektedir. Ne var ki, bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu ile korunan tek hukuki yararın bireyin malvarlığı değeri olduğu da söylenemez. Bununla beraber, söz konusu düzenleme ile kişilerin bilişim sistemlerine olan güvenlerinin de korunduğu, dolayısıyla bu norm ile birden çok hukuki değerin koruma altına alındığını söylememiz mümkündür[29].

C) SUÇUN MADDİ UNSURU

Ceza hukukunda suç, her şeyden önce bir fiilden ibarettir. Bu fiilin oluşumu için de, yapma veya yapmama biçiminde dış dünyada somutlaşacak bir davranışın söz konusu olması gerekir. Ancak, insan davranışının ceza hukuku bakımından dikkate değer olarak kabul görmesi için, bir sonucunun olması, yani olgular dünyasında somut bir değişiklik meydana getirmesi ve elbette bunların da arasında birbirleriyle bağını ispatlayacak bir nedensellik bağının mevcut bulunması gerekir. İşte davranış, sonuç ve nedensellik bağından oluşan bu bütüne *"maddi unsur"* adı verilmektedir[30].

TCK m. 244/1'in düzenlemesi uyarınca *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."* Buna göre, ilgili suç seçimlik hareketli bir suç olup, bu seçimlik hareketler "*bir bilişim sisteminin işleyişinin engellenmesi*" ve "*bir bilişim sisteminin işleyişinin bozulması*"dır. Bu maddedeki "*engelleme*", bilişim sisteminin çeşitli yollarla geçici olarak durdurulması[31], söz gelimi, sistemin olması gerekenden daha yavaş çalışması, işlevini kendinden beklendiği gibi yerine getirememesi, veri alışverişi yapamaması, veri işleme hızının düşmesi gibi halleri ifade etmektedir[32]. Hükümdeki "*bozulma*"yı ise, sistemin veri işleme faaliyetini hiçbir şekilde yapamayacak hale getirilmesi[33]

[29] **Bayraktar ve diğerleri**, s. 255; **Veli Özer Özbek/ Koray Doğan/Pınar Bacaksız/İlker Tepe**, Türk Ceza Hukuku Özel Hükümler, Ankara, 2018, s. 975. Bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunun hukuki konusuna ilişkin tartışmalar ve farklı görüşler için bkz. **İrem Geçmez**, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244), Ankara, 2020, s. 76-79.

[30] **Francesco Antolisei**, Manuale di Diritto Penale, Parte Generale, Milano, 2003, s. 220-221; **Zeki Hafızoğulları/ Muharrem Özen**, Türk Ceza Hukuku Genel Hükümler, Ankara, 2012, s. 193; **Toroslu/Toroslu**, s. 131.

[31] **Dönmezer**, s. 623; **Geçmez**, s. 82.

[32] **Bayraktar ve diğerleri**, s. 259.

[33] **Ketizmen**, s. 129.

olarak anlamak mümkündür. Sistemin işleyişinin daimî veya geçici olarak yahut belirli bir süre için veya sürekli olarak çalışmaması suçun oluşumu için önemli değildir. Engelleme veya bozulma kısa süreli de olsa TCK m. 244/1'deki suç meydana gelecektir[34].

Bilişim sistemleri nazara alındığında, bu sistemlerin esas özelliklerini klavyesi, monitörü, faresi gibi fiziksel varlıklarını oluşturan *donanım*ından çok, işlemcisi, verileri, programları, sunucusu gibi soyut varlıklarını ihtiva eden *yazılım* unsuru belirlemektedir. Ancak, bahsi geçen yazılım unsurunun doğru bir biçimde çalışması, örneğin verilerin işlenmesi ya da saklanması, donanım unsurunun da işlevini yerine getirmesini sağlamaktadır. İşte birbirine bağlı olarak işleyen bu süreç, kanun koyucu tarafından "*bilişim sisteminin işleyişi*" olarak formüle edilmiştir[35].

Bilişim sistemi hem somut hem de soyut varlıkları ifade ettiğinden ve bunların işlemesi birbirine bağlı olduğundan, bunlardan birisine yapılan müdahale diğer unsuru da temelden etkilemektedir. Bu itibarla, sistemin maddi varlığını oluşturan donanıma yönelik fiziksel saldırılar da bu madde kapsamında olup, bunun şartı ise bahsi geçen fiziksel saldırının amacının bilişim sisteminin işleyişine yönelmesidir[36]. Buradan hareketle, bilişim sisteminin işleyişine yönelmeyen donanıma yönelik fiziksel saldırılar, TCK m. 244/1 kapsamında değerlendirilmeyecektir. Örneğin, sistemin işleyişini engelleme amacı gütmeden bir bilgisayara fiziksel saldırıda bulunan fail TCK m. 244/1'den değil, TCK m. 151'deki "*Mala Zarar Verme*" suçundan sorumlu olacaktır[37]. Bu bağlamda, sisteme müdahale suçunun maddi unsurunu, bir bilişim sisteminin işleyişinin engellenmesine yönelmiş, o bilişim sisteminin donanımına veya yazılımına yapılan saldırılar olarak tanımlamak mümkündür. Bunun yanı sıra, söz konusu fiilin meydana getiriliş şekli de suçun oluşumu açısından önemsizdir. Suçu oluşturan fiiller direkt olarak bilişim sistemine saldırıda bulunmak suretiyle işlenebileceği gibi, dolaylı yollarla, söz gelimi sisteme veri iletim ağı yoluyla virüs yazılımı gönderilerek de işlenebilir. Her iki durumda da failin TCK m. 244/1 uyarınca ceza sorumluluğu doğacaktır[38].

Bu fiil, teknolojik gelişmelerin artmasına paralel bir biçimde, sınırsız sayıda yöntemle gerçekleştirilebilir. Örneğin, bir web sayfasına erişim, genel olarak o web sayfasını barındıran sunucu bilgisayara (*hosting*) bağlantı

[34] **Bayraktar ve diğerleri**, s. 260.
[35] **Ketizmen**, s. 133.
[36] **Kurt**, s. 165.
[37] **Özbek/Doğan/Bacaksız/Tepe**, s. 963; **Geçmez**, s. 85.
[38] **Dülger**, s. 403.

kurulması ve sunucuda bulunan web sayfasının içeriğinin yer aldığı verinin kopyalanması anlamına gelmektedir. Web sayfasının yer aldığı sunucu ise, belli bir zaman diliminde, ancak belli sayıda bağlantı sağlayabilecek ve veri kopyalamasına izin verebilecek bir kapasiteye sahiptir. Sunucunun bu kapasitesine de "*bant genişliği*" adı verilmektedir. İşte, bu sunucunun birim zamandaki işlem kapasitesinin aşılmasını sağlayacak şekilde ve bu amaçla sistemle bağlantı kurulması yönünde gönderilecek çok sayıda talep, sistemin taleplere cevap verememesini ve kilitlenmesine sebep olacaktır. Bu durumda web sayfasına erişim sağlanamayacak ve söz konusu bilişim sisteminin işleyişi engellenecektir[39].

Konuyu açıklığa kavuşturmak amacıyla bir örnek daha vermemiz yerinde olacaktır: Kurum işlerini yürütmek üzere yüklenmiş bir yazılımı kullanan bir kurum bilgisayarını düşünelim. Kurum içi bir ağ vasıtasıyla bu bilgisayar kurum içerisindeki diğer bilgisayarla veri iletişimini sağlamakta, yaptığı işlemleri iletmekte olsun. Söz konusu kurum bilgisayarının bir bilişim sistemi olduğu hususunda hiçbir şüphe yoktur. Bu bilişim sistemi, kendini çalıştıran bir işletim yazılımına (*örneğin, Windows işletim sistemine*) sahiptir. Aynı zamanda da, kurum içi faaliyetlerini yürütebilmek için kurum tarafından yazdırılan bir programı kullanmaktadır. Kullanılan bu program da bilişim sisteminin soyut bir unsurudur. Saldırganlar, ağ üzerinden sisteme ulaşsalar, ana bilgisayara yüklü halde bulunan kurum yazılımının kodlarını değiştirseler ve bu değişiklik sebebiyle söz konusu bilgisayarı kullanan memur iş yapamaz, evrak gönderemez ve veri transferi yapamaz hale gelse, bu durumda bilişim sisteminin bozulması söz konusu olacaktır. Failler, yazılımın kodlarını değiştirerek sistemin işleyişini bozmaktadırlar. Bu durumda kurum yazılımı ile işlem yapamayan memurun, bilgisayarında yüklü diğer işletim sistemi Windows üzerinden müzik dinliyor ya da film seyredebiliyor olması, suçun oluşumuna etki etmeyecektir. Aynı örnekte, faillerin kurumun uygulama programına değil, bahsi geçen bilgisayarı hedef aldıklarını düşünelim. Failler bilgisayarda kurulu bulunan işletim sistemine ait bir kısım dosyayı tahrip etseler, bu kez de sistem dosyaları tahrip olduğundan bilgisayar çalışmayacaktır. Tekrar çalışabilmesi içinse, işletim sisteminin baştan kurulması gerekecektir. Burada da bilişim sisteminin bozulmasından bahsetmek gerekmektedir. Bu arada hiç dokunulmayan kurumun diğer bilgisayarlarının veya kurum yazılımının çalışıyor olması, suçun oluşumuna etki etmeyecektir. Aynı şekilde, fail sistemin işleyişini engellemek için fiziki

[39] **Ketizmen**, s. 134-135.

olarak bilgisayarları kırsa da, yine bilişim sisteminin işleyişini bozma suçu meydana gelecektir[40].

Bunun dışında, sistemin engellenmesi ve bozulmasına yönelik sonsuz sayıda örnek verilebilir. Bu şekilde tamamen yazılıma yönelik yapılacak saldırılar da, örneğin sistemin engellenmesine yönelik olarak bir bilgisayarın işlemcisi, anakartı gibi donanımına verilecek fiziksel zararlar da, TCK m. 244/1'in maddi unsurunu oluşturacaktır. Ancak şunu unutmamak gerekir ki, ister donanıma fiziksel zarar verilsin ister yazılım unsuruna müdahale edilsin, fiil ile bilişim sisteminin işleyişine zarar verilmesi amaçlanmış ve bu sonuç meydana gelmişse, TCK m. 244/1'deki suçun maddi unsuru; buna karşın bilişim sistemine yönelik bir amaç güdülmeksizin donanıma yapılacak fiziksel müdahalelerde ise TCK m. 151'deki "*Mala Zarar Verme*" suçunun maddi unsuru meydana getirilmiş olacak ve fail bu hüküm uyarınca cezalandırılacaktır.

Suçun maddi unsurunu oluşturan bir diğer husus ise "*sonuç*"tur. Sonuç, hareket veya ihmalden kaynaklanan ve doğalcı anlamda dış dünyada bir etki yaratan her türlü davranış olarak tanımlanabilir[41]. Bu tanımdan hareketle dış dünyada bir sonuç meydana getiren suçlara "*sonuç suçları*", dış dünyada herhangi bir etki doğurmayan suçlara ise "*sonuçsuz suçlar*" veya "*sırf hareket suçları*" adı verilir. TCK m. 244/1'de düzenlenen suçun neticesinde bilişim sisteminin işleyişinin engellenmesi veya bozulması sonucu meydana geldiğinden, bu suçların "*sonuçlu suçlar*" kapsamında olduğu kuşkusuzdur.

Sonuçlu suç ve sırf hareket suçu ayrımından başka, suçun sonuçları bakımından yapılan bir başka ayrım "*zarar suçu*" ile "*tehlike suçu*" ayrımıdır. Suçun tamamlanması anı esas alınarak failin suçu oluşturan fiilinin hukuken korunan varlık veya menfaati zarara uğrattığı, tahrip ettiği veya azalttığı suçlara "*zarar suçları*", buna karşılık, korunan varlık veya menfaati yalnızca tehlikeye soktuğu suçlara *"tehlike suçları"* adı verilmektedir[42]. Örneğin, kasten insan öldürme (TCK m. 81) veya kasten yaralama (TCK m. 86) suçları birer zarar suçuyken; suçu ve suçluyu övme (TCK m. 215), tehdit (TCK m. 106) veya inşaat veya yıkımla ilgili emniyet kurallarına uymama (TCK m. 176) gibi suçlar hukuken korunan menfaat açısından sadece tehlike yarattığından birer tehlike suçudur. Doktrinde bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunun tehlike suçu mu yoksa zarar suçu mu olduğu hususunda bir görüş birliği bulunmamaktadır. Ancak bu tartışmalara

---

[40] **Kurt**, s. 165-166.
[41] **Toroslu/Toroslu**, s. 141.
[42] **Antolisei**, s. 264-265; **Toroslu/Toroslu**, s. 144.

girmeksizin belirtmeliyiz ki[43], TCK m. 244/1'deki suçun meydana gelmesi için, tipik fiildeki "*bilişim sisteminin işleyişinin engellenmesi veya bozulması*" neticesinin oluşması zorunlu olduğundan ve dolayısıyla norm ile korunan hukuki menfaat zarara uğradığından, söz konusu suç bir zarar suçudur.

D) SUÇUN MANEVİ UNSURU

TCK m. 21 uyarınca "*Suçun oluşması kastın varlığına bağlıdır. Kast, suçun kanunî tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesi*" iken, m. 22'ye göreyse "*Taksirle işlenen fiiller, kanunun açıkça belirttiği hâllerde cezalandırılır. Taksir, dikkat ve özen yükümlülüğüne aykırılık dolayısıyla, bir davranışın suçun kanunî tanımında belirtilen neticesi öngörülmeyerek gerçekleştirilmesidir."* Bu hükümler bağlamında TCK'nın manevi unsur sistemine göre, suçun varlığı için kural olarak kastın bulunması gereklidir. Buna karşın, kasıt olmaksızın da bir kimsenin cezalandırılacağı, bunun için o kimsenin taksirle hareket etmesi gerektiği, ancak failin taksir nedeniyle cezalandırılabilmesi için, ilgili suçu düzenleyen kanun hükmünde taksire ilişkin açık hükmün bulunması gerektiği öngörülmektedir[44].

Bu itibarla, bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunun manevi unsurunun kasıt olduğu hususunda hiçbir şüphe bulunmamaktadır. TCK m. 244 bakımından taksirli sorumluluk hali düzenlenmediğinden, bu suçun taksirle işlenebilmesi mümkün değildir. O halde, sisteme müdahale suçu nedeniyle cezalandırılabilmesi için, failin hedef bilişim sisteminin işleyişini engellemek veya bozmak fiilini bilerek ve isteyerek gerçekleştirmesi gerekmektedir[45].

Burada önem arzeden husus, yukarıda da açıkladığımız üzere, failin mutlaka "*bilişim sisteminin işleyişini engelleme veya bozma*" sonucuna yönelmesi ve bu kasıtla hareket etmesi gerekliliğidir. Bu açıklamanın özel kasıt olarak düşünülmemesi gerekir. Zira kanun koyucu 244/1. maddede herhangi bir özel amaç yahut saik aramadığından, suçun meydana gelmesi için genel kasıt yeterli olacaktır[46]. Bilişim sisteminin işleyişine yönelmeden, yalnızca maddi zarar vermek için bir bilgisayarın donanımına saldıran, örneğin bilgisayarın ana kartını kıran failin fiilinde bilişim sisteminin

[43] Bu tartışmalar için bkz. **Geçmez**, s. 85-86.
[44] **Toroslu/Toroslu**, s. 229; **Hafızoğulları/Özen**, s. 276.
[45] **Değirmenci**, s. 205; **Kurt**, s. 175.
[46] **Geçmez**, s. 96.

işleyişini engelleme veya bozma kastı değil mala zarar verme kastı bulunduğundan, fail TCK m. 244/1 değil, mala zarar verme suçunu düzenleyen TCK m. 151 nedeniyle sorumlu olacaktır.

D) SUÇA ETKİ EDEN NEDENLER

Suça etki eden nedenler adı verilen durumların somut olayda bulunması halinde, nitelikli suçtan söz edilir. Bu bakımdan, suça etki eden neden, suçun ağırlığını etkileyen, bir başka deyişle suçun daha ağır veya hafif hale gelmesi ve dolayısıyla suçun basit şekline ait cezanın değişmesi sonucunu doğuran yahut aktif süjenin suça eğiliminin belirtilerini ortaya koyan nedendir[47].

TCK m. 244'ün üçüncü fıkrasında suçun nitelikli haline yer verilmiştir. Buna göre;

"Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

Üçüncü fıkradaki bu ağırlaştırıcı neden, birinci fıkradaki sisteme müdahale ve ikinci fıkradaki veriye müdahale fiillerinin bir kamu kurum ya da kuruluşuna ait bilişim sistemi üzerinde işlenmesinin daha vahim sonuçlar doğurabileceğinden bahisle, verilecek cezayı yarı oranında arttırmaktadır. Doktrinde bu hususun ağırlaştırıcı neden olarak düzenlenmesinin sebebini, kişisel bilgisayarlara müdahale sonucu ortaya çıkan zarar ile kamu kurum veya kuruluşlarının bilgisayar sistemlerine müdahale sonucu ortaya çıkan zarar arasında büyük farklar olmasına dayandıran yazarlar bulunmaktadır[48].

TCK'nın 244. maddesinin dördüncü fıkrasında ise, ayrı bir suç olarak "*haksız çıkar sağlama*" fiili düzenlenmiştir. Bu düzenlemeye göre;

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

Her ne kadar bu fiil ayrı bir suç olarak düzenlenmiş ise de, hükümde öngörülen sonucun ortaya çıkması birinci veya ikinci fıkrada sayılan fiillere bağlandığından, bu suça da kısaca değinmemiz gerekmektedir. Bu hükümde, yine sisteme veya veriye müdahale fiillerinin işlenerek kişilerin bundan haksız yarar sağlaması üzerine, bunun başka bir suça vücut vermemesi halinde, cezanın ağırlaştırılacağı söylenmektedir. Söz konusu düzenlemenin

[47] **Toroslu/Toroslu**, s. 279.
[48] Bkz. **Dülger**, s. 243.

bir "*tali norm*" niteliğinde olduğu kuşkusuzdur. Kanun koyucunun bu hükümde bahsi geçen "*başka bir suç*"tan kastı, büyük ölçüde dolandırıcılık, hırsızlık veya güveni kötüye kullanma gibi suçlardır. Örneğin, TCK m. 157'de dolandırıcılık suçunun oluşumu bakımından hile unsuru öngörüldüğünden, eğer bilişim sistemleri aracılığıyla kişinin kendisi veya başkasına haksız yarar sağlamasında bir hile kullanması durumunda dolandırıcılık suçu, hile kullanmaksızın söz konusu fiili gerçekleştirmesi durumunda ise TCK m. 244/4'teki haksız çıkar sağlama suçu meydana gelecektir.

Ne var ki, bir kişiye karşı hile yapılmaksızın bilişim sistemlerinin kullanılarak haksız yarar sağlanmasının nasıl tespit edileceği yahut bir başka deyişle hile ile bilişim sistemlerinin kullanılmasıyla haksız çıkar sağlanmasının uygulamada nasıl ayırt edileceği tartışma konusudur. Bu husus, 765 sayılı Mülga TCK'nın 525/b maddesinin yürürlükte olduğu dönem de tartışmalara konu olmuş ve Yargıtay tarafından birçok kez birbirinden farklı kararlar verilmiştir. Örneğin, Yargıtay bir kararında, *"Sanık ...'nın, müdür yardımcısı ...'nın başka bir amaçla verdiği şifreyi haksız olarak kullanmak suretiyle, mevduat sahiplerinin hesaplarında vade başı ve vade sonu bilgileri ile faiz oranlarını değiştirerek, oluşturduğu faiz farkını, Nazmiye adına açtığı menkul hesabı ile Sabri adına açılan vadesiz hesaba ve kendi adına açtığı vadesiz tasarruf ve menkul hesaba aktarmak, bir kısmını da nakden çekmek suretiyle inceleme tarihi itibariyle ... lirayı haksız olarak mal edindiği..."* fiilin dolandırıcılık olduğu kanaatine varmış[49]; bir başka kararında ise *"... Hizmetli olarak çalıştığı bankanın bilgisayar sistemine girerek usulüne uygun açılmış bir maaş kredi limitli bankomat hesabının kredi limitini yükseltmek ve ayrıca kendi adına usulsüz olarak bankomat 7/24 hesabı açmak suretiyle haksız yarar sağladığı oluşa uygun olarak kabul edilen sanığın eyleminin TCK'nın 525/b maddesinin 1. Fıkrasındaki suça uygun bulunduğu*" gerekçesiyle, benzer bir fiili sisteme müdahale suretiyle haksız yarar sağlamak olarak değerlendirmiştir[50]. Oysa her iki kararda da, herhangi bir kimse yönünden hile söz konusu olmayıp, söz konusu fiiller, bilişim sisteminin kullanılması ile kişilerin kendilerine haksız yarar sağlamalarından ibarettir. Kanun koyucunun anladığı anlamdaki "hile" ile bilişim sistemlerini iyi kullanan faillerin fiilleri arasındaki ayrım halen net bir şekilde çizilebilmiş olmayıp, failin ceza sorumluluğunu belirleyecek kadar

[49] **Yargıtay CGK, 11.3.2003, E. 2002/11-329, K. 2003/29**.
[50] **Yargıtay 11. CD, 2.12.1997, E. 1997/5052, K. 1997/6536**.

önemli olan bu hususa ilişkin yargıda ve doktrinde bir mutabakat sağlanmış değildir[51].

Suça etki eden nedenler arasında, suçun terör amacıyla işlenmesinin de sayılması gerekmektedir. Bu nitelikli hal TCK'da değil, 3713 sayılı Terörle Mücadele Kanunu'nda ("*TMK*") düzenlenmiştir. TMK'nın 4. maddesinde "*aşağıdaki suçlar 1 inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır*" denilerek, bu suçlar arasında TCK'nın 244. maddesi de sayılmıştır. Bu düzenlemeye göre, bir bilişim sisteminin işleyişinin engellenmesi veya bozulması fiili bir terör örgütünün faaliyetleri kapsamında ve TMK'nın 1. maddesinde tanımlanan "terör amacı" çerçevesinde işlenirse, terör suçu sayılacaktır[52].

Bu suçun terör suçu sayılması halinde, muhakemesi ve infazında TMK'daki hükümler uygulama alanı bulacağı gibi, ayrıca TMK'nın 5. maddesi uyarınca, tayin edilecek hapis cezaları veya adli para cezaları yarı oranında arttırılacak ve bu suretle tayin olunacak cezalarda gerek o fiil için gerekse de her nevi ceza için belirlenmiş cezanın yukarı sınırı aşılabilecektir.

E) SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ

1. Teşebbüs

5237 sayılı TCK'nın 35. maddesinde teşebbüs şu şekilde düzenlenmiştir: "*Kişi işlemeyi kastettiği suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise, teşebbüsten dolayı sorumlu tutulur*"

Teşebbüse gerçek anlamda karakterini veren husus, söz konusu tanımdaki "*elverişli hareketlerle icraya başlayıp da elinde olmayan nedenlerle tamamlayamama*" ölçütüdür. Teşebbüs aşamasında kalmış bir suçun maddi

[51] Buna ilişkin tartışmalar ve değerlendirmeler için Bkz. **Ketizmen**, s. 168-175.

[52] TMK'nın 1. maddesinde "terör" şu şekilde tanımlanmış olup, bu nitelikli halin meydana gelmesi için bilişim sisteminin işleyişinin engellenmesi veya bozulması fiili ancak bu kapsamda işlenirse terör suçu olduğu kabul edilecektir:
"Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir."

unsuru, elverişli hareketlerle doğrudan doğruya icraya başlama ancak suçu elinde olmayan nedenlerle tamamlayamama, manevi unsuru ise suç işleme kastıdır. Bu itibarla, teşebbüs derecesinde kalmış bir suçun cezalandırılabilmesi için teşebbüsün kurucu unsurlarının tamamının somut olayda gerçekleşmiş olması gerekmektedir. Bununla beraber şunu da söylememiz gerekir ki, teşebbüs bakımından önem arzeden husus failin suç kararının dış dünyaya yansıması ve algılanabilir biçimde bir davranışta somutlaşmasıdır, aynı zamanda hazırlık hareketleri aşamasından çıkıp icra hareketleri kapsamına girmesi gerekmektedir. Dolayısıyla, cezalandırılabilir teşebbüsü tespit etmek için yalnızca faildeki suç işleme kastını ve maddi unsuru değil, failin suç işleme kastının dış dünyaya yansıması ve icra hareketi şeklinde tezahür eden davranışı incelemek gerekmektedir[53].

Bir suça teşebbüsün söz konusu olabilmesi için önemli koşullardan biri de, suçu meydana getiren icra hareketlerinin bölünebilir olmasıdır. Bu açıdan neticesi harekete bitişik suçlar yönünden, başka bir deyişle failin hareketi gerçekleştirir gerçekleştirmez tamamlanan suçlar yönünden teşebbüs söz konusu olmazken, icra hareketleri parçalara bölünebilir suçlara teşebbüs mümkündür[54]. Sonuçlu suçları meydana getiren icra hareketleri kural olarak bölünebilir olduklarından, bu suçlara teşebbüsün mümkün olduğu kabul edilmektedir.

Bilişim sisteminin işleyişinin engellenmesi veya bozulması suçuna da teşebbüs mümkündür. Buna göre, bilişim sisteminin işleyişinin engellenmesi veya bozulması sonucunu gerçekleştirmeye yönelik hareketlerin tamamlanamadığı veya hareket tamamlanmış dahi olsa tipik fiilde öngörülen sonucun meydana gelmediği hallerde suçun teşebbüs aşamasında kaldığı kabul edilecek ve faile verilecek ceza TCK'nın 35. maddesine göre tatbik edilecektir[55].

TCK'nın 36. maddesinde 'Gönüllü Vazgeçme' kurumu düzenlenmiştir. Bu maddeye göre, "*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*."

---

[53] **Giuseppe Bettiol**, Diritto Penale, Parte Generale, Padova, 1976, s. 535; **Ferrando Mantovani**, Diritto Penale, Parte Generale, Padova, 2001, s. 455; **Gürkan Özocak**, Türk Ceza Hukukunda Suça Teşebbüs, Ankara, 2018, s. 64-65 **(Suça Teşebbüs)**.

[54] **Mantovani**, s. 465-466; **Özocak**, Suça Teşebbüs, s. 224.

[55] **Bayraktar ve diğerleri**, s. 266.

Buna göre, TCK m. 36, gönüllü vazgeçme durumunda faile o suçtan ceza verilmeyeceğini, ancak fiilin tamam olan kısmı bir suça vücut veriyorsa, failin o suçtan cezalandırılacağını öngörmektedir. Örneğin, bir kimsenin evine hırsızlık maksadıyla giren fail, hırsızlık suçunu işlemeden fiilini sonlandırırsa, TCK m. 36 uyarınca hırsızlık suçundan sorumlu olmayacak, ancak vazgeçme anına kadarki fiilleri neticesinde TCK m. 116'da düzenlenen konut dokunulmazlığını ihlal suçu meydana geldiğinden yalnızca bu suçtan dolayı cezalandırılacaktır[56]. Gönüllü vazgeçmenin bilişim sisteminin işleyişinin engellenmesi veya bozulması fiilleri yönünden de uygulama alanı bulacağı açıktır. Söz gelimi, sistemin işleyişini engelleyici bir davranışta bulunmak üzere bir bilişim sistemine giren, ancak sonrasında bu davranışından vazgeçen fail TCK m. 244/1'e teşebbüsten cezalandırılmayacak, ancak o ana kadarki fiili TCK m. 243'te düzenlenen bilişim sistemine girme suçuna vücut verdiğinden, TCK m. 243/1'den sorumlu olacaktır[57].

Burada TCK'nın 244. maddesinin dördüncü fıkrasında düzenlenen "*haksız çıkar sağlama*" suçuna ayrıca değinmemiz gerekmektedir. Bu suç da bir zarar suçu olduğundan, 244. maddenin birinci fıkrasındaki fiili icrasının tamamlanamadığı veya icrası tamamlanmasına karşın dördüncü fıkrada suçun oluşumu için öngörülen haksız çıkarın sağlanamadığı hallerde, bu suçun teşebbüs aşamasında kaldığı kabul edilecektir. Ancak bunun için failin kastının yalnızca birinci fıkradaki neticeyi gerçekleştirmek değil, aynı zamanda haksız çıkar sağlamayı da kapsaması gerekecektir[58]. Bununla birlikte, fail birinci fıkradaki fiili tamamlar ve fakat haksız çıkar sağlamaktan gönüllü olarak vazgeçerse, 36. madde düzenlemesi uyarınca TCK m. 244/4'teki suçtan sorumlu olmayacak, yalnızca o ana kadar gerçekleştirdiği TCK m. 244/1'deki fiilinden dolayı cezalandırılacaktır.

---

[56] Doktrinde, TCK m. 36'daki "*icra hareketleri sonrası gönüllü vazgeçme*" düzenlemesi eleştirilmiş ve düzenlemenin kusur sorumluluğu ilkesi ile çeliştiği söylenmiştir. Örneğin, fail öldürme kastıyla bir kişiyi bıçaklamış, ancak daha sonra pişman olarak o kimsenin ölmesini engellemiştir. Burada, TCK'nın düzenlemesine göre, icra hareketleri sonrası gönüllü vazgeçme vardır ve fail cezalandırılmaz. Ancak, tamamlanan kısım yaralama suçunu meydana getirdiğinden, fail yaralama suçundan cezalandırılacaktır. Ne var ki, bu olayda failin kastı yaralama değil, öldürmedir. Bu durumda, yaralama kastı olmaksızın hareket eden bir kimsenin fiili için yaralamadan ceza verildiği takdirde, kanun gerekçesinde kesin bir şekilde reddedilen objektif sorumluluk esasına göre karar verilmiş olacağı söylenmiştir. Bkz. **Hafızoğulları/Özen**, s. 343.

[57] **Geçmez**, s. 101.

[58] **Bayraktar ve diğerleri**, s. 266-267.

2. İştirak

Bir kişi tarafından işlenebilen bir suçun, birden fazla kişi tarafından önceden işbirliği yapılarak gerçekleştirilmesine iştirak adı verilmektedir[59]. Esasen ceza kanunlarında öngörülen suç tipleri, bazı istisnai haller dışında, tek bir kişi tarafından işlenmeleri göz önünde bulundurularak düzenlenmektedirler. Ne var ki, somut olayda, tek bir kişi tarafından işlenmesi mümkün olan ve dahası ceza normunda da bu şekilde düzenlenmiş olan suç tiplerinin birden fazla kişinin katkısı veya etkisi ile işlenmesi mümkündür. İştirake ilişkin kurallar, bir kişi tarafından işlenebilen bu suç tiplerinin, birden fazla kişinin katılması, etkide veya yardımda bulunması suretiyle işlenmeleri durumunda, bu suçun işlenmesine iştirak eden diğer ortakların ceza sorumluluklarının nasıl belirleneceği meselesini düzenlemektedir[60].

Suça iştiraki düzenleyen ceza normları TCK'nın dördüncü bölümünde 37 ilâ 40. maddeler arasında yer almaktadır. Buna göre, Türk ceza hukukunda suça iştirakin türleri temelde iki kategoride düzenlenmiş olup, bunlar "*faillik*" ve "*suç ortaklığı*" şeklinde adlandırabilir. Birinci kategori olan "*faillik*" TCK'nın 37. maddesinde *doğrudan faillik*, *müşterek faillik* ve *dolaylı faillik* olarak üçe ayrılmıştır. Doğrudan fail ile bu faille birlikte hareket ederek fiil üzerinde hakimiyet kuran müşterek fail ve bir başkasını araç olarak kullanmak suretiyle suçun işlenmesini sağlayan dolaylı fail, kanuni tanımda öngörülen cezanın tamamından sorumludur. Suç ortaklığı ise, *azmettirme* ve *yardım etme* olarak iki alt başlıkta incelenebilir. Azmettirme, TCK'nın 38. maddesi uyarınca, bir kimsenin aklında o suçu işlemek olmamasına rağmen o suçu işlemesini sağlayan ortak olarak, işlenen suçla ilgili kanun hükmünde belirlenen ceza ile cezalandırılır. Buna karşın TCK'nın 39. maddesinde yardım etme, iştirakin diğer türlerine göre suça daha az yoğunlukta bir katılma olarak öngörülmüş olup; buna göre, *"bir kimseyi suç işlemeye teşvik etmek", "suç işleme kararını güçlendirmek", "fiilin işlenmesinden sonra yardımda bulunacağını vaat etmek", "suçun nasıl işleneceği hususunda yol göstermek"* veya *"fiilin işlenmesinde kullanılan araçları sağlamak"* yahut *"suçun işlenmesinden önce veya işlenmesi sırasında yardımda bulunarak suçun icrasını kolaylaştırmak"* şeklinde vuku bulmakta ve yardım etmek

[59] **Devrim Aydın**, Türk Ceza Hukukunda Suça İştirak, Ankara, 2009, s. 23; **Sulhi Dönmezer/Sahir Erman**, Nazari ve Tatbiki Ceza Hukuku, Cilt: II, İstanbul, 1987, s. 481 **(C. II)**.

[60] **Timur Demirbaş**, Ceza Hukuku Genel Hükümler, Ankara, 2019. s. 499.

suretiyle bir suça iştirak edene, suç tipini düzenleyen normdaki ceza miktarından belli oranlarda indirim yapılarak ceza verilmektedir[61].

TCK m. 244/1'de düzenlenen suçun iştirak halinde işlenmesi mümkündür. Bu suç iştirak açısından herhangi bir özellik göstermemektedir. Örneğin, bir kimsenin bilişim sisteminin işleyişini bozucu bir virüsün gönderilmesini fiilini müşterek olarak işleyen kimseler TCK m. 37 uyarınca müşterek fail olarak cezalandırılacaklar, bir kişinin bu fiili işlemek hiç aklında yokken onu bu fiili işlemeye azmettiren, örneğin ikna eden yahut para veren kimse TCK m. 38 uyarınca azmettirici olarak aynı ceza sorumluluğuna sahip olacak, bu fiili işleyen failin fiili işlemesini kolaylaştıran, onu teşvik eden veya yol gösteren kimse ise TCK m. 39 uyarınca yardım eden sıfatıyla cezalandırılacaktır.

3. İçtima

Ceza hukukunda somut olayda işlenen suç sayısını, dış dünyada meydana gelen sonuç belirlemektedir. Buna göre, kanuni tanıma uygun olarak gerçekleştirilen her sonuç, kural olarak, ayrı ve bağımsız bir suça vücut vermekte olup, fail hareketi ile ne kadar sonuç meydana getirmişse o kadar suç işlemiş olmakta ve her bir suç yönünden ayrı ayrı cezalandırılmaktadır[62]. Ne var ki, bazı durumlarda, fail tarafından gerçekleştirilen fiil birden çok kanun hükmünü yahut farklı fiiller birden çok kez aynı kanun hükmünü ihlal etmiş olabilir. Bu durumlara ceza hukukunda "*suçların içtimaı*" veya "*suçların kaynaşması*" adı verilmektedir[63].

Ceza hukuku açısından "*fiil*" hareket ile neticenin birlikte ele alınmasını ifade etmektedir. Bu nedenle somut olayda failin hareketinin tekliği veya çokluğu fiilin tekliği yahut çokluğu bakımından bir etki doğurmayacak, ortaya çıkan doğalcı anlamdaki neticeye göre fiil sayısı belirlenecektir[64]. Ceza hukukunda kanun koyucu bazı hallerde birden çok ihlali tek suç saydığı ve faile tek bir ceza verilmesini emrettiği içtima halleri öngörmüş olup, bu içtima halleri *bileşik (mürekkep) suç, zincirleme (müteselsil) suç* ve *fikri içtima* olarak ortaya çıkmaktadır.

---

[61] Suça iştirakin türleri ve buna ilişkin görüşler hakkında detaylı açıklama için bkz. **Aydın**, s. 130 vd.; **Demirbaş**, s. 503 vd.; **Dönmezer/Erman**, C. II, s. 482 vd..

[62] **Dönmezer/Erman**, C. II, s. 403; **Hafızoğulları/Özen**, s. 376.

[63] **Demirbaş**, s. 540.

[64] **Dönmezer/Erman**, C. II, s. 403.

Bileşik suç TCK'nun 42. maddesinde düzenlenmiş olup, "*biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir.*" Türk Ceza Kanunu'nda düzenlenen bilişim suçları yönünden bileşik suçtan söz etmek mümkün değildir. Bu nedenle, çalışmamızın konusunu oluşturan bilişim sisteminin işleyişinin engellenmesi veya bozulması fiili yönünden ele alınacak ilk içtima kurumu zincirleme suçtur. Zincirleme suç, TCK'nın 43. maddesinde şu şekilde düzenlenmiştir: "*Bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir. Ancak bu ceza, dörtte birinden dörtte üçüne kadar artırılır. Bir suçun temel şekli ile daha ağır veya daha az cezayı gerektiren nitelikli şekilleri, aynı suç sayılır*." Bu açıklamaya göre zincirleme suçu, kasıttan ayrı olarak, failin kurguladığı bir suç işleme planı dahilinde, aynı suçu aynı kişiye karşı birden çok kez gerçekleştirmesi olarak tanımlamak mümkündür[65]. Maddenin ikinci fıkrası uyarınca "*aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi"* de zincirleme suç kapsamında sayılmakta ve faile bu hüküm uyarınca tek bir ceza verilmektedir.

TCK'nun 244/1. maddesinde düzenlenen bilişim sisteminin işleyişinin engellenmesi veya bozulması fiilinin zincirleme suçun konusu olması mümkündür. Nitekim bu fiil, bir suç işleme kararının icrası kapsamında, değişik zamanlarda aynı kişiye karşı birden fazla kez işlendiğinde zincirleme suç söz konusu olacak ve TCK m. 43 uyarınca faile tek suçtan dolayı verilecek ceza arttırılacaktır. Ne var ki burada "*tek suç işleme kararının icrası*"nın doğru bir şekilde değerlendirilmesi ve tespit edilmesi gerekmektedir. Eğer failin icra hareketleri arasında tek bir suç işleme kararından söz edilemeyecek denli uzun aralıklar mevcutsa, zincirleme suç söz konusu olmayacak ve faile her bir fiilinden dolayı ayrı ayrı ceza verilecektir[66]. Aynı şekilde, bu suç tek bir fiille birden fazla kişiye karşı işlendiğinde de TCK'nın 43. maddesindeki zincirleme suç hükmü uygulama alanı bulacaktır.

İçtima bakımından ele alınması gereken bir diğer kurum ise fikri içtimadır. TCK'nın 44. maddesinde öngörülen fikri içtima hükmü uyarınca, "*işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır*." Fikri içtimanın söz konusu olabilmesi için sonuç odaklı bir değerlendirme yapılması gerekmektedir. Buna göre, failin fiili ile ortaya çıkan sonuç tek ise fiilin de

[65] **Hafızoğulları/Özen**, s. 381.
[66] **Dülger**, s. 410.

tek olduğu, buna karşın sonuç birden fazla ise fiilin de sonuç sayısı kadar olacağı kabul edilmelidir. Dolayısıyla dış dünyada meydana gelen tek bir somut değişiklik halinde "*tek fiil*" söz konusu olduğundan fikri içtimanın uygulanabileceği, ancak dış dünyada birden fazla somut neticenin meydana gelmesi halinde ortada sonuç sayısı kadar fiil olacağından fikri içtimadan bahsedilemeyeceği kanaatindeyiz[67]. Buna göre, fikri içtimanın söz konusu olabilmesi için fail tarafından olgular dünyasında meydana gelmiş tek bir fiil gerçekleştirilmesi ve bu tek fiil ile birden farklı ceza normunun aynı anda ihlal edilmiş olması gerekmektedir. Örneğin, başkasına ait bir özel belgenin yok edilmesi olayında, fail tek bir fiil ile hem mala zarar verme (TCK m. 151), hem de belgeyi yok etme (TCK m. 208) suçunu işlemektedir[68]. Bu örnekte, failin dış dünyaya yansıyan iradesi tek olduğundan ve doğalcı anlamda tek bir sonuç meydana geldiğinden, faile her iki ceza normu nedeniyle ceza verilmemekte ve fikri içtima hükmü dolayısıyla bu suçlardan cezası daha ağır olan uygulanmaktadır.

Bir bilişim sisteminin işleyişinin engellenmesi veya bozulması fiilini işleyen fail, bu fiili ile aynı zamanda başka bir ceza normunu da ihlal ediyorsa, fikri içtimadan söz etmek mümkündür. Örneğin, fail bilişim sisteminin işleyişini bozmak amacıyla doğrudan bir donanıma saldırıyor, bunu parçalıyor ve bu sayede bilişim sisteminin işleyişini bozuyorsa, tek bir fiil ile TCK'nun 244/1. maddesindeki suç ile 151. maddesindeki mala zarar verme suçu oluşacaktır. Bu durumda, TCK m. 44 uygulanacak ve iki suçtan daha ağır ceza öngörülen TCK m. 244/1'deki bilişim sisteminin işleyişinin bozulması suçundan faile ceza verilecektir[69].

Somut olayda bir fail tarafından birden fazla bilişim suçu da işlenebilir. Örneğin, bir fail sisteme girmeksizin veri nakillerini izlerken bir süre sonra sistemin içine girerek sistemin işleyişini engelleyebilir veya bilişim sisteminin işleyişini bozmak için bir virüs üreten bir fail sonrasında bu virüsü kullanarak gerçekten sisteme zarar verebilir. Bu durumlarda failin tek bir fiilinden değil birden çok fiilinden bahsetmek gerekeceğinden ceza hukukunda "*gerçek içtima*" dediğimiz husus söz konusu olacak ve faile iki

---

[67] Aynı görüşte bkz. **Erem**, s. 363; **Dönmezer/Erman**, C. II, s. 416; **Toroslu/Toroslu**, s. 369; **Mustafa Özen**, "*Ceza Hukukunda Fikri İçtima*", Türkiye Barolar Birliği Dergisi, Sayı: 73, 2007, s. 139-140**.**

[68] **Toroslu/Toroslu**, s. 370.

[69] **Geçmez**, s. 106. Bu durumda, mala zarar verme suçu ile bilişim sisteminin işleyişinin bozulması suçunun farklı hukuki konulara sahip olduğunu, dolayısıyla iki suçla farklı menfaatlerin ihlal edildiğini, aralarında genel – özel norm ilişkisinden bahsedilemeyeceğini savunan yazarlar da bulunmaktadır. Bkz. **Dülger**, s. 411.

suç fiilinden ayrı ayrı ceza verilecektir. Yukarıdaki örneklerden ilkinde fail TCK m. 243/4 ve m. 244/1'de, ikincisinde ise TCK m. 244/1 ile m. 245/A'da düzenlenen suçlardan ayrı ayrı cezalandırılacaktır.

E) UYGULAMADA SIK GÖRÜLEN BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME VEYA BOZMA SALDIRILARI

Bilişim suçları ve bu suçların işlenmesinde kullanılan yöntemler, teknolojik gelişme alanları genişledikçe, buna paralel olarak gelişmekte, çoğalmakta ve farklılaşmaktadır. Bu nedenle bu saldırıları sınıflandırmamız veya sınırlandırmamız pek mümkün görünmemektedir[70]. Bunun yanı sıra, bilişim suçlarında ve saldırılarda kullanılan teknik yöntemler birden farklı aşamada da gündeme gelebilmektedir. Söz gelimi, bilgisayar virüsleri hem sisteme sızma hem de izlerin yok edilmesi aşamalarında kullanılabilmektedir[71]. Bu nedenle bilişim sisteminin işleyişinin engellenmesi veya bozulması saldırılarını tek tek saymak mümkün değilse de, çalışmamızın bu bölümünde uygulamada çok sık görülen hizmet aksatma ve bilişim sistemine müdahale saldırı türlerinden *DoS ve DDoS saldırıları, tavşanlar (rabbits)* ve *SPAM*'ler üzerinde durulacaktır. Bunun yanı sıra, klasik bir siber saldırı türü olan *hacking* yöntemiyle, ayrıca *Botnet* veya *Phsihing* gibi saldırı metotlarıyla da bir bilişim sisteminin güvenlik duvarı aşılarak sistemin ele geçirilmesi ve bunun ardından sistemin içerisinden işleyişinin engellenmesi veya bozulması da mümkündür[72]. Ne var ki bu bölümde, doğrudan sistemin hizmetini aksatmaya yönelen ve buna özgülenen saldırı türlerinden söz edilecektir.

1. DoS ve DDoS Saldırıları

TCK m. 244/1 bağlamında, bilişim sistemine müdahale fiillerinin en sık görülen yöntemi DoS *(Denial of Service)* ve DDoS *(Distributed Denial of Service)* saldırılarıdır. DoS saldırısı, kısaca, belli bir sunucunun belli bir şekilde hizmet bekleyen kullanıcılara hizmet verememesini sağlamak

[70] Siber saldırı yöntemlerinin tarihçesi ve bunlara ilişkin sosyo kültürel araştırmalara ilişkin detaylı bilgi için bkz. **Mesut Orta**, Bilişim Suçları ve Elektronik Delillerin Toplanması, Muhafazası, Değerlendirilmesi, Sunulması, Ankara, 2015, s. 87 vd.
[71] **Karagöz**, s. 98.
[72] Diğer siber saldırı yöntemleri hakkında açıklama için bkz. **Dülger**, s. 120 vd.; **Orta**, s. 101 vd.; **Mustafa Altınkaynak**, Uygulamalı Siber Güvenlik ve Hacking, 5. Baskı, İstanbul, 2018, s. 5 vd.

amacıyla, o bilgisayarın işlem yapmasını engellemek, bir başka deyişle hedef bilgisayarı bilişim sisteminin içerisine girmeksizin kilitlemektir. DoS işlemi, birden çok sayıda bilgisayar üzerinden yapıldığında, yani "*dağıtık*" (*distributed*) bir şekilde gerçekleştirildiğinde ise ortaya DDoS saldırısı çıkmaktadır[73]. Uygulamada en sık görülen bilişim sistemine müdahale fiillerinden biri DDoS saldırısıdır.

DDoS saldırısında, saldırgan, *hacking* yoluyla daha önceden ele geçirmiş ve hazırlamış olduğu birçok makina üzerinden veya BOT IP'ler üzerinden, seçmiş olduğu hedef sistemin trafiğini arttırarak, o sistemin işleyemez hale gelmesini sağlamaktadır. Saldırganın *hacking* yoluyla ele geçirmiş olduğu ve görünürde hedef bilgisayarların sistemlerine saldıran bu makinalara "*zombi*" adı verilir. *Zombi*ler esasen saldırganın daha önce bir açığını bularak ele geçirdiği (*hacklediği*) ve saldırı sırasında kullanmak üzere içlerine program yerleştirdiği bilgisayarlardır. Bir başka deyişle, *zombi*ler saldırının merkezinde bulunan, ancak saldırı fiilinden haberdar dahi olmayan ve güvensiz olduğu için saldırgan tarafından ele geçirilmiş makinalardır. *Zombi* programları, genellikle güvenliği zayıf olan sistemlere yerleştirilmektedir.

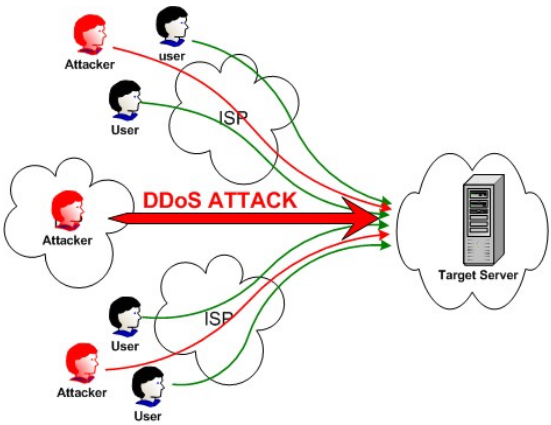
Saldırgan tarafından *zombil*er üzerinde kurulan programlar (*daemon*) belirli bir kaynaktan gelecek DDoS komutlarını dinlemekte ve bu yolla hedef sisteme saldırıları gerçekleştirmektedir. Binlerce sisteme yerleştirilen bu programlar, bilgisayarlara uzaktan kontrol (*remote*) olanağı vermekte, böylece saldırganın bu bilgisayarlar üzerinden istediği *server*'a (*sunucu*) istediği sayıda veri göndererek o *server*'ı çalışamaz hale getirmesine olanak sağlamaktadır[74].

İfade ettiğimiz gibi saldırgan, bu *zombi* bilgisayarları veya BOT IP'leri kullanarak hedef olarak belirlediği sisteme (bilgisayara ya da *hosta*) aynı anda giriş yapmaya çalışmakta ve bu yolla kapasitesinin çok üzerinde istek gelen sistem tamamen kilitlenerek çalışamaz hale gelmektedir. Örneğin, barındırma hizmeti veren bir firmadan belirli bir bant genişliği edinen ve buna göre azami olarak aynı anda iki bin kişinin girebileceği bir web sitesine, aynı anda ikiyüz bin kişinin girmeye çalıştığı ve girmeye çalışırken bu ikiyüz bin kişinin ayna anda komut yolladığı durumda, bu web sitesine ulaşılması mümkün olmamaktadır. İşte DDoS saldırısında, aynı anda binlerce kişinin belli bir sisteme sürekli giriş yapmaya çalışması gibi, bu işi otomatize eden bir yazılımla hedef sistem kilitlenmekte ve çalışamaz duruma getirilmektedir.

---

[73] **Karagöz**, s. 110.

[74] **Gürkan Özocak**, "*DDoS Saldırısı ve Failin Cezai Sorumluluğu*", Bilişim 2012 – 29. Uluslararası Bilişim Kurultayı Bildiriler Kitabı, Ankara, 2012, s. 24 **(DDoS Saldırısı).**



Şekil 1. DDoS Saldırı Şeması[75]

Yukarıdaki şemadan da görülebileceği üzere, DDoS saldırısında hedef sunucuya (*target server*), aynı anda çok sayıda istek gelmekte olup, sistemin kaynakları (*CPU, Stack, band vs*.) bu yoğun istekleri karşılayamadığı durumda, sisteme gerçek kullanıcılar (*user*) tarafından da erişilmesi imkânsız hale gelmektedir. Sistemin kilitlenmesi durumu, *zombi* bilgisayarların çokluğuna ve gelen isteklerin yoğunluğuna bağlı olarak, saatler sürebilmekte olup, sisteme gelen yükün azalıp sisteme girişin kabul edilebilir seviyeye inmesine kadar devam edebilmektedir.

Koordineli ve sistematik bir biçimde yapılan bu işlem, hem saldırının yoğunluğunun artmasına, hem de gerçek saldırganın kimliğinin gizlenmesine yol açmaktadır. Zira, saldırılar *zombi* bilgisayarlar üzerinden yapıldığından, saldırı yapan bilgisayara ulaşılmak istenildiğinde *zombi* bilgisayarların IP adresleriyle karşılaşılmakta ve teknik olarak saldırıya katılmayan gerçek saldırgana ulaşmak mümkün olmamaktadır. Saldırı tek bir IP adresi üzerinden yapıldığında bir *Firewall* (*güvenlik duvarı*) bunu rahatlıkla önleyebilecekken, daha çok sayıdaki IP adresinden saldırı yapılması, *log* taşması nedeniyle *Firewall* servislerini durdurmakta ve *Firewall*'un devre dışı kalmasına neden olmaktadır. İşte DDoS saldırılarını, tek bir IP adresi üzerinden gelen DoS saldırılarından ayıran en önemli fark buradan kaynaklanmaktadır. DDoS saldırılarında, saldırgan çok sayıdaki *zombi* bilgisayarı veya IP'yi hedef sisteme yönlendirdiğinden *Firewall* devre dışı kalmakta ve saldırının

[75] **Özocak**, DDoS Saldırısı, s. 25.

yoğunluğuna bağlı olarak önlenmesi kimi zaman imkânsız hale gelmektedir[76].

DDoS saldırısında, hedef sisteme aynı anda çok sayıda bilgisayar üzerinden istek gönderildiğinden, sistem kilitlenmekte ve çalışamaz hale gelmektedir. Böylece, saldırgan esasen sistemin içine girmeksizin veya herhangi bir veriye müdahale etmeksizin, yalnızca sisteme erişilmesini engellemektedir. Bu itibarla, DDoS saldırısının, TCK m. 244/1 kapsamında "*bilişim sisteminin işleyişinin engellenmesi*" suçuna vücut verdiği şüphesizdir.

Ne var ki, uygulamada esas sorun, yukarıda açıkladığımız *zombi*lerin ceza sorumluluğu bakımından ortaya çıkmaktadır. Çünkü, somut olaya bakıldığında, TCK m. 244/1'deki suçun maddi unsuru görünüşte *zombi* bilgisayarlar tarafından, iştirak halinde meydana getirilmektedir. Zira, bu bilgisayarlar hedef bilişim sistemine çok sayıda istek göndererek sistemin kilitlenmesine ve işleyişinin engellenmesine sebep olmaktadırlar. Bu nedenle uygulamada "delilden faile gidilmesi" prensibi uygulandığında, ulaşılan sonuç *zombi* bilgisayarların IP adresleri veya doğrudan BOT IP'ler olmaktadır[77]. Ancak bunlar yalnızca saldırgan tarafından yönlendirilen ve ceza hukuku açısından "*longa manus*" (*uzun el*) adı verilebilecek araçlar olup, bunlara ceza verilemeyeceği gibi, bunlar üzerinden faile ulaşmak da çoğu kez mümkün olmayacaktır. Dolayısıyla, DDoS saldırılarında mevcut delillerden veya suçun neticelerinden yola çıkılarak asıl failin tespit edilmesi oldukça zordur.

2. Tavşanlar (Rabbits)

Tavşan adı verilen yazılımlar, son derece çabuk üreyebilen ve içine girdikleri bilişim sisteminin içinde işlemciye anlamsız ve sürekli komutlar vererek işlemcinin bilişim sisteminin normal işleyişini sağlayan komutları vermesini engelleyen veya yavaşlatan ve sistemin daha yavaş çalışmasına sebep olan, sonunda da sistemi çalışmaz hale getirerek kilitleyen yazılımlardır[78].

Tavşanlar bir kez sistemin içine girdikten sonra faaliyete geçebilmeleri için ayrıca bir komuta yahut dışarıdan bir müdahaleye ihtiyaç duymayan

[76] DDoS saldırı yöntemleriyle ilgili ayrıntılı bilgi için Bkz. **Özocak**, DDoS Saldırısı, s. 24-26.

[77] Zombi sistemlerinin oluşturduğu bu sisteme BotNet (Bot Ağı) da denilmektedir. Bkz. **Karagöz**, s. 111.

[78] **Dülger**, s. 114.

kötücül yazılımlardır. Bunlar sisteme girip çalışmaya başladıktan sonra işlemciye sürekli yük bindirmekte, diskte yer alan tüm alanı doldurmakta ve bir süre sonra sistemi tamamen işlemez hale getirmektedirler. Bu özellikleriyle sisteme içeriden ve kendiliğinden DDoS saldırısı yapıyormuş gibi bir çalışma prensibine sahiptirler[79].

Günümüzde tavşan yazılımları, bir sistemin işleyişini yavaşlatmak ve bozmak amacıyla olduğu kadar, işlemcinin sahibinden farklı komutlar vererek o kimseyi küçük düşürmek veya başkalarıyla onun adına iletişime geçiyormuş izlenimi vermek, bu yolla fidye almak vb. birçok farklı amaçla kullanılabilmektedir[80].

3. SPAM'ler

Spam sözcüğü esasen ABD menşeli Hormel Foods Corporation'ın ürettiği gıdalarla ilgili bir kısaltmadır ve "*spiced pork and ham*" (*baharatlı domuz ve jambon*) ibaresinin baş harflerinden oluşmaktadır[81]. Ne var ki Spam, bilişim dünyasında istem dışı gönderilen e-postalara verilen genel bir isim olarak benimsenmiş ve zamanla bir siber güvenlik sorunu haline gelmiştir.

E-posta ile iletişim hayatımıza girdiği ilk günden itibaren, kullanım kolaylığı ve sınırsızlığı ile hayatımızın vazgeçilmezlerinden olmuşsa da, bu durum özellikle yığın halinde gönderilen e-postalar nedeniyle yavaş yavaş bir sorun haline de gelmiştir. İstenmeyen e-postalar, bir süre sonra kişilik haklarına müdahale noktasına gelmiş ve yaygın hak ihlalleri arasında yerini almıştır[82]. Zira bir kimsenin e-posta kutusuna gelen binlerce e-postanın hangisinin gerçek veya gerekli hangisinin gereksiz (*spam*) olduğunu tespit etmek son derece güç olup, bu gereksiz e-postaların şikâyet edileceği bir kurum da bulunmamaktadır. Bazı firmaların veri tabanlarındaki bazen yüzbinleri hatta milyonları bulan e-postaları satmaları, bilgisayar korsanlarının (*hacker*) yaptıkları aktif ya da pasif aramalarla elde ettikleri veriler, site içerisinde veya farketmeden onay verilen çerezler aracılığıyla e-

---

[79] **Karagöz**, s. 112.

[80] Örneğin, yakın tarihte Rusya merkezli ortaya çıkan **'Kötü Tavşan'** (Bad Rabbit) isimli bir tavşan yazılımının, 'Adobe Flash Player' güncellemesi görünümlü sahte bir yazılımla (virüs ile) kullanıcıların bilgisayarlarına sızdığı, bu yolla sistemi ele geçirdiği ve verilerin teslim edilip sistemin eski hale getirilmesi için sistemin sahibinden bu yolla fidye istendiği tespit edilmiştir. Bkz. https://www.cnnturk.com/teknoloji/bilgisayarlarda-yeni-tehdit-kotu-tavsan?page=5 (erişim tarihi: 31.07.2023)

[81] **Dülger**, s. 117.

[82] **Orta**, s. 100.

posta adresi tarayan ve kaydeden yazılımlar gibi sorunlar da istenmeyen e-postaların çoğalmasına sebebiyet vermektedir[83]. Buna dair ABD başta olmak üzere çeşitli ülkelerde yasama çalışmaları yapılmaktadır[84].

Spam ile ilgili en önemli sorunlardan birisi, İnternet trafiğini olumsuz yönde etkilemesi ve özel olarak e-posta trafiğini kilitlenecek noktaya getirmesidir. Öyle ki, bir süre sonra gerçek e-postaların spam olanların arasında bulunması dahi mümkün olmamakta, böylece sorun haberleşme özgürlüğünün kısıtlanması noktasına kadar gitmektedir. Spam e-postaların hizmet veya İnternet yahut e-posta akışını yavaşlatmak ya da aksatmak amacıyla gönderilmesi halinde ise, bu fiilin artık TCK'nın 244/1. maddesi bağlamında bilişim sisteminin işleyişinin engellenmesi veya bozulması suçuna vücut vereceği açıktır[85].

IV. SONUÇ

Son yıllarda ciddi anlamda gelişme ve ilerleme gösteren teknolojik devinim ve buna paralel olarak artan bilgisayar kullanımı ile beraber, toplumun yaşayış biçimi ve dolayısıyla suç ve suçluluğun zemini de değişmiştir. Bu bağlamda, "*klasik suçlar*" olarak adlandırılan suçların yanı sıra, "*bilişim suçları*" adı verilen bir grup suç da ülkelerin ceza kanunlarında kendine yer bulmaya başlamıştır.

Toplumun ve teknolojik olanak ve ihtiyaçların gelişmesiyle doğru oranda artış gösteren bilişim suçları, hali hazırdaki klasik suçlardan kategorik olarak farklı suçları kapsamamış, bilakis bu suçların bilişim sistemlerinin sosyo-ekonomik dönüşüm içerisinde ceza hukukuna etkisi ortaya çıkmış, bu bakımdan bu suçlar bir ihtiyaç olarak ceza kanunlarında düzenlenirken, bir yanda gerek kategorik, gerekse pratik sebeplerle kimi sorunlar ve tartışmalar yaratmıştır[86].

Çalışmamızın kapsamını aşan bu tartışmalar bir yana bırakıldığında, ilk defa 1991 tarihli 3765 sayılı Kanunla 765 sayılı Türk Ceza Kanunu'na giren bilişim suçları, 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nun 243-246 maddeleri arasında, "Topluma Karşı Suçlar" arasında, Kanunun Üçüncü Kısmının 10. Bölümünde "Bilişim Alanında Suçlar" başlığıyla düzenlenmiştir. Bu yeni düzenlemeyle, "Bilişim Alanında Suçlar" "*Yetkisiz Erişim", "Sisteme Müdahale", "Veriye Müdahale (Değiştirme,*

[83] **Karagöz**, s. 112.
[84] Bu yasama çalışmaları hakkında bilgi için bkz. **Dülger**, s. 118; **Orta**, s. 101.
[85] **Geçmez**, s. 41; **Karagöz**, s. 112.
[86] **Ketizmen**, s. 243.

Bozma, Yok Etme, Erişilmez Kılma)", "Bilişim Sistemleri Aracılığıyla Yarar Sağlama" ve *"Banka ve Kredi Kartlarının Kötüye Kullanımı*" olarak öngörülmüştür.

Çalışmamızın konusunu oluşturan "Bilişim Sisteminin İşleyişini Engelleme veya Bozma Suçu", 5237 sy. TCK'nun 244/1. maddesinde düzenlenmiştir. Seçimlik hareketli bir suç olarak öngörülen TCK m. 244/1, hem "*bilişim sisteminin işleyişinin engellenmesi",* hem de "*bilişim sisteminin işleyişinin bozulması*" fiillerini kapsamaktadır. Bu fiillerin, bilgisayarın donanımına yapılan fiziki müdahaleleri kapsamadığı, yalnızca yazılımlara yönelik müdahaleleri kapsadığı görüşleri ortaya atılmaktaysa da, kanımızca "*bilişim sisteminin engellenmesi veya bozulması*" amacıyla ve bu sonuç irade edilerek bir bilgisayarın fiziki donanımına yönelik gerçekleştirilen saldırıların da TCK m. 244/1 bağlamında değerlendirilmesi gerekmektedir.

Bunun yanında, sisteme müdahale suçunun uygulamada en sık görülen yöntemi DoS ve DDoS saldırısı olarak adlandırılan saldırı (*hacking*) yöntemidir. Bu yöntemde, failler, hedef olarak belirledikleri bilişim sisteminin hiçbir şekilde içine girmeksizin, daha önce güvenlik zafiyetinden faydalanarak ele geçirdikleri ve *zombi* adı verilen yüzlerce, hatta binlerce bilgisayarı yahut BOT kaynakları hedef sisteme yönlendirerek ve bu sisteme çok sayıda istek göndererek, sistemin bunlara cevap verememesine ve çalışamaz hale gelmesine sebep olmaktadırlar. Görünüşte saldırıyı yapan *zombi* bilgisayarlar olduğundan ve yapılacak incelemede *zombi*lerin IP adreslerine ulaşılacağından, esas saldırgana ulaşmak neredeyse imkânsız olmakla beraber, saldırganın fiilinin TCK m. 244/1 bağlamında sisteme müdahale olduğu tartışmasızdır. Bunun yanı sıra, uygulamada *tavşan (rabbit)* yazılımlar veya *spam* gibi yöntemlerin de kullanıldığı ve ayrıca çok sayıda *hacking* yöntemi kullanılarak gerçekleştirilen farklı siber saldırı türleriyle de karşılaşıldığı görülmektedir.

Özellikle bilişim sisteminin işleyişine yönelen veya hizmet aksatma amacı güden saldırılarda TCK m. 244/1'in uygulanması söz konusu olacağı açıktır. Ne var ki, siber suçlulukla mücadelede ceza sorumluluğunun belirlenmesi kadar, siber risklerin önceden tespit edilmesi, bilişim sistemlerini siber saldırı risklerinden koruyucu tedbirlerin alınması, özellikle enerji, ulaştırma, telekomünikasyon, finans gibi önemli ve kritik hizmet veren sektörlerde bilişim sistemlerin bu tür saldırılardan korunabilmesi için belirli hukuki ve teknik gereksinimler belirlenmesi gibi önleyici tedbirlerin öngörülmesi de elzemdir. Ülkemizde bu yönde çeşitli çalışmalar yapılmakta ve elektronik haberleşme gibi bazı sektörlerde buna dair ikincil düzenlemeler bulunmakta ise de, genel olarak güçlü bir mevzuatın bulunduğunu söylemek güçtür.

V. KAYNAKÇA

Ali Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara, 2005.

Ali Osman Özdilek, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul, 2006.

Berrin Bozdoğan Akbulut, "*Bilişim Suçları*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, Sayı: 1-2, Cilt: 8, Konya, 2000, s. 545-555.

Devrim Aydın, Türk Ceza Hukukunda Suça İştirak, Ankara, 2009.

Faruk Erem, "*Bilgisayar Suçları ve TCY*", Yargıtay Dergisi, Cilt: 17, Sayı: 4, Ekim 1991.

Faruk Erem, Ümanist Doktrin Açısından Türk Ceza Hukuku, C. I, Ankara, 1987.

Ferrando Mantovani, Diritto Penale, Parte Generale, Padova, 2001.

Francesco Antolisei, Manuale di Diritto Penale, Parte Generale, Milano, 2003.

Giuseppe Bettiol, Diritto Penale, Parte Generale, Padova, 1976.

Gürkan Özocak, "*DDoS Saldırısı ve Failin Cezai Sorumluluğu*", Bilişim 2012 – 29. Uluslararası Bilişim Kurultayı Bildiriler Kitabı, Ankara, 2012, s. 23-29.

Gürkan Özocak, Türk Ceza Hukukunda Suça Teşebbüs, Ankara, 2018.

Hans-Heinrich Jescheck, Alman Ceza Hukukuna Giriş, Çev. Feridun Yenisey, İstanbul, 2007.

İrem Geçmez, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244), Ankara, 2020.

Hasan Sınar, İnternet ve Ceza Hukuku, İstanbul, 2001.

Kubilay Taşdemir/ Ramazan Özkepir, Mala Karşı Suçlar, Ankara, 1993.

Köksal Bayraktar/Zeynel T. Kangal/Ali Hakan Evik/Pınar Memiş Kartal/Fulya Eroğlu/Vesile Sonay Evik/Ali Kemal Yıldız/Eylem Aksoy Retornaz/Gülşah Bostancı Bozbayındır/Asuman Aytekin İnceoğlu, Özel Ceza Hukuku, Ekonomi, Sanayi ve Ticarete İlişkin Suçlar – Bilişim Alanında Suçlar, Cilt VIII, İstanbul, 2021.

Levent Kurt, Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.

Mehmet Can Karagöz, Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, İstanbul, 2020.

Mesut Orta, Bilişim Suçları ve Elektronik Delillerin Toplanması, Muhafazası, Değerlendirilmesi, Sunulması, Ankara, 2015.

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

Muharrem Özen/İhsan Baştürk, Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011.

Murat Volkan Dülger, Bilişim Suçları, Ankara, 2004.

Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, 2014.

Mustafa Altınkaynak, Uygulamalı Siber Güvenlik ve Hacking, İstanbul, 2018.

Mustafa Özen, "*Ceza Hukukunda Fikri İçtima*", Türkiye Barolar Birliği Dergisi, Sayı: 73, 2007, s. 132-145.

Nevzat Toroslu/Haluk Toroslu, Ceza Hukuku Genel Kısım, Ankara, 2019.

Nevzat Toroslu, Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Ankara, 1970.

Olgun Değirmenci, "*2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi*", Türkiye Barolar Birliği Dergisi, Sayı: 58, Ankara, 2005

Salvatore Resta, Computer Crimes Tra Informatica e Telematica, Cedam, 2000.

Sulhi Dönmezer, Kişilere ve Mala Karşı Cürümler, İstanbul, 2001.

Sulhi Dönmezer/Sahir Erman, Nazari ve Tatbiki Ceza Hukuku, Cilt: I, İstanbul, 1987.

Sulhi Dönmezer/Sahir Erman, Nazari ve Tatbiki Ceza Hukuku, Cilt: II, İstanbul, 1987.

Timur Demirbaş, Ceza Hukuku Genel Hükümler, Ankara, 2019.

Ulrich Sieber, "*Bilgi Toplumunda Ceza Hukuku ve Dijitalleşme – Bilişim Suçları*", Çeviren: Prof. Dr. Feridun Yenisey – Av. Damla Zaimoğlu, Bilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku, Ankara, 2021.

Veli Özer Özbek/ Koray Doğan/Pınar Bacaksız/İlker Tepe, Türk Ceza Hukuku Özel Hükümler, Ankara, 2018.

Yılmaz Yazıcıoğlu, Kriminolojik, Sosyolojik ve Hukuki Boyutları İle Bilgisayar Suçları, İstanbul, 1997.

Zeki Hafızoğulları/ Muharrem Özen, Türk Ceza Hukuku Genel Hükümler, Ankara, 2012.