Bilişim Sistemine Girme ya da Sistemde Kalma Suçu

Ahmet BÜKE*

Bu makale hakem incelemesinden geçmiştir ve TÜBİTAK – ULAKBİM Veri Tabanında indekslenmektedir.

* Avukat, İzmir Barosu, (bukeahmet@hotmail.com)
ORCID ID: 0000-0001-9515-9003.

Makale geliş tarihi: 27 Eylül 2021 **Makale kabul tarihi:** 29 Eylül 2022

Atıf önerisi: Büke, Ahmet. "Bilişim Sistemine Girme ya da Sistemde Kalma Suçu." Ankara Barosu Dergisi 80, no. 4 (Ekim 2022): 33-80.
DOI: 10.30915/abd.1186640

BİLİŞİM SİSTEMİNE GİRME YA DA SİSTEMDE KALMA SUÇU

ÖZ

Bilim ve teknolojinin baş döndürücü hızla gelişimine paralel olarak bilişim hukuku alanında ülkemizde ve dünyada hukuki düzenleme yapma zorunluluğu doğmuştur. Günümüzde dijital iletişim araçlarının kullanımının yaygınlaşması ile bilişim sistemine girme ya da bilişim sisteminde kalma fiilleri, herkes tarafından kolayca işlenebilecek bir suç türü konumundadır. Bu suç, başta bilişim sisteminin güvenliği ve güvenilirliği olmak üzere kişisel veriler, kişilerin özel yaşamı, ticari alan, ulusal ve uluslararası güvenlik gibi birçok alanı tehdit edebilecek konuma geldiği için temel bir bilişim suçudur. Bu çalışmada Türk Ceza Kanunu'nun 243. maddesinde yer alan "Bilişim Sistemine Girme ya da Sistemde Kalma" suçu, uygulamadan örnekler sunularak yargı kararları ışığında analiz edilmiştir.

Anahtar kelimeler

bilişim | sistem | teknoloji | bilişim sistemine girme ya da sistemde kalma suçu | TCK m. 243

THE CRIME OF ACCESSING DATA PROCESSING SYSTEM AND REMAINING WITHIN THE SYSTEM

ABSTRACT

Parallel to the dizzying development of science and technology, it has become necessary to make legal arrangements in the field of informatics law in our country and the world. Today, with the widespread use of digital communication tools, the acts of entering or staying in the information system are a type of crime that can be easily committed by anyone. This crime is a basic IT crime because it has come to a position that can threaten many areas such as personal data, private life, commercial area, national and international security, especially these security and reliability of the information system. In this study, the crime of accessing data processing system and remaining within the system, which is regulated in Article 243 of the Turkish Penal Code, has been analyzed in the light of judicial decisions by presenting examples from the application.

Keywords

informatics | system | technology | the crime of accessing data processing system and remaining within the system | article 243 of the Turkish Penal Code

GİRİŞ

Bilim ve teknolojinin baş döndürücü hızla geliştiği çağımızda bilişim sistemi olarak kabul edilebilecek program ve yazılımlar, sürekli olarak güncellendiği için bu sistemler de yaşamımızın ayrılmaz bir parçası konumuna gelmiştir.[1] Teknolojik yenilikler karşısında bilişim sistemlerinin güvenliği ve güvenilirliği de ciddi anlamda sorgulanmaktadır. Çünkü, sosyal medya kullanımının yaygınlaşması, pandeminin de etkisi ile eğitim, ticaret ve bankacılık işlemleri de dahil bir çok faaliyet, bu sistemler kanalı ile yürütülmektedir. Ayrıca devletler de bilişim sistemlerinde, ulusal güvenliğe dayalı gizli bilgiler ile vatandaşlara ait kişisel pek çok veriyi, bilişim sistemlerinde saklamaktadır. Buna bağlı olarak teknolojinin sağladığı hız ve olanaklar her ne kadar büyük bir kolaylık sağlasa da sistemde kullanılan verilerin üçüncü şahıslar tarafından ele geçirilip istismar edilme olasılığı, sistemin güvenliği yönünden ciddi bir tehdit oluşturmaktadır. Bu durumun etkisi ile bilişim sistemlerinde işlenen ya da bilişim sistemleri aracılığıyla işlenen bu fiiller, ceza hukukunun uygulama alanına sokulmuştur.

Bilişim alanında yaşanan yenilikler ve gelişmeler, hukuk alanında da önemli bazı sorunlara yol açmaktadır. Dolayısıyla bu alanda yaşanan gelişmelerle birlikte fikri hak, haksız fiil, mülkiyet, özel hayat gibi önem arz eden hukuksal kavramların tanımları ile anlayış biçimleri değişmiştir. Buna bağlı olarak 5237 sayılı TCK'nin 243. maddesinde düzenlenen bilişim sistemine girmek ya da orada kalmaya devam etmek suçu, uygulamada sıkça karşılaşılan bir suç tipidir.

Çalışmamızda öncelikli olarak bilişim kelimesinin anlamından yola çıkarak bilişim suçlarının kaynağı ve bu suç özelinde bilişim sistemlerine girme ve kalma suçlarına genel olarak değinilecek, sonrasında bu suçla korunan hukuki değer irdelenecektir.

Çalışmada; suçun faili ve mağduruna yer verildikten sonra bilişim sistemine girme suçunun unsurları suç sistematiğine uygun olarak incelenecektir. Bu çerçevede suçun maddi unsurları, manevi unsur, hukuka aykırılık unsuru ayrıntılı olarak ele alınacaktır. Bunun dışında suçun nitelikli halleri ile neticesi sebebiyle ağırlaşmış haline değinilecek, ardından kusurluluğa

[1] Özge Sırma Gezer ve Yasemin Filiz Saygılar Kırıt, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)," *Fasikül Hukuk Dergisi 11*, no. 111, (İstanbul: Şubat 2019): 429.

ilişkin bazı hususlar ve suçun özel görünüş biçimleri, ayrıntılı şekilde ele alınacaktır. Daha sonra bilişim sistemine girme ya da sistemde kalma suçuna uygulanan yaptırım konusuna yer verilecek ve sonuç bölümünde konuya ilişkin izlenimler ile çalışma noktalanacaktır.

I. GENEL OLARAK

Bilişim sözcüğünün etimolojik kökenini, Fransızca "informatique" kelimesi oluşturmaktadır. Bu sözcük, Türkçe'ye "enformasyon" şeklinde çevrilerek kullanılmıştır;[2] ancak, bu sözcüğün kullanımı uzun sürmemiş ve enformasyon yerine Türkçe karşılığı bilişim kelimesi kullanılmaya başlanmıştır. *İnformatique* sözcüğü, bilgi vermek anlamına gelmektedir. Dolayısıyla yabancı kökenli bir kelime yerine, bilgi kökeninden türemiş olan "bilişim" sözcüğünün kullanılması isabetli bir tercih olmuştur. Bu kelime, sözlük anlamı olarak "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi"* olarak tanımlanmaktadır.[3]

Bilişim, insanların teknik, ekonomik, sosyal ve toplumsal alanlarda iletişimde kullandığı bilginin, özellikle bilgisayar aracılığıyla sistemli ve düzenli biçimde işlenmesi sonucu her tür bilginin, yapay olarak yeniden üretilmesidir. Bunun sonucu olarak bilgi, bilgisayarlarda depolanmakta ve kullanıcıların erişimine hazır hale getirilmektedir.[4] Böylece bilişim hem verilerin işlenmesini hem de bu işlem sonuçlarının aktarılmasını yani veri içeriğini de kapsayan bir kavramdır.[5]

Bilişim alanında yaşanan yenilikler ve gelişmeler, hukuk alanında da önemli bazı sorunlara yol açmaktadır. Dolayısıyla bu alanda yaşanan gelişmelerle birlikte fikri hak, haksız fiil, mülkiyet, özel hayat gibi önem arz eden hukuksal kavramların tanımları ile anlayış biçimleri değişmiştir. Sözgelimi

[2] Caner Yenidünya ve Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,* (İstanbul: Legal Yayınevi, 2003), 27.

[3] Yenidünya ve Değirmenci, *Bilişim Suçları*, 29.

[4] Berrin Akbulut, "Bilişim Suçları," *Selçuk Üniversitesi Hukuk Fakültesi Dergisi 8,* no. 1-2, (*Milenyum Armağanı* 2000): 545.

[5] Yenidünya ve Değirmenci, *Bilişim Suçları*, 29.

fikri hak konusunda yazılıma ilişkin ürünler üzerindeki haklar bakımından marka ve patent hakkı ortaya çıkmıştır. Bu hakların içeriğinin izinsiz olarak kullanılmasına bağlı olarak haksız fiil kavramı, yeni bir boyut kazanmıştır. Bunun sonucu olarak sosyal medya hesaplarında bilişim sistemlerine kaydedilen bilgilere izinsiz ulaşılması ve bunların rıza dışı kullanılması, özel hayatın gizliliğini ihlal suçunu oluşturmaktadır.[6]

Bilişim kavramına ceza hukukunda ilk kez 1989 tarihli Türk Ceza Kanunu Ön Tasarısı'nda yer verilmiştir. Bu tasarıda bilişim alanı; bilgilerin toplanıp depo edilmesinin ardından bunların otomatik işleme tabi tutulduğu sistem şeklinde tanımlanmıştır. Bu tanıma765 sayılı mülga Türk Ceza Kanunu'nda 1991 yılında yapılan değişiklik sonrasında 3756 sayılı kanunun gerekçesinde de yer verildiği görülmektedir.[7]

Bilişim suçu kavramı, bilişim teknolojisinde çağımızda yaşanan gelişmelerle ceza hukuku alanında ortaya çıkmış ve kendisine özgü özellikleri olan bir kavramdır[8]. Bu suçlar ifade edilirken doktrinde çeşitli kavramların kullanıldığı görülmektedir. Bunlar arasında, "siber suç" (*cybercrime*), elektronik suç (*electronic crime*), dijital suç (*digital crime*) ve çoğunlukla da bilgisayar ya da bilişim suçları (*computer-related crime*) terimlerinin kullanıldığı görülmektedir.[9]

Günümüzde bilişim teknolojisinin gelişimi ile birlikte gelişmiş batı ülkelerinin çoğunda belgeleme ve veri elde etme tekniğinin üst düzeye ulaşmasına paralel olarak bilişim ayrı bir disiplin olarak algılanmaya başlamıştır. Bunun sonucu olarak insanların gündelik yaşantılarında sahip oldukları ekonomik, sosyal, teknik ve hukuki verilerin saklanması, saklanan bu verilerin gerektiğinde işlenmesi gerekmektedir. İştebilişim sistemi olarak da adlandırılan

[6] Hakan Karakehya, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu," *Türkiye Barolar Birliği Dergisi* 81, (2009): 14.

[7] Yenidünya ve Değirmenci, *Bilişim Suçları,* 28.

[8] Ali Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*, 5. Baskı, (Ankara: Seçkin Yayıncılık, 2014), 53.

[9] Yenidünya ve Değirmenci, *Bilişim Suçları*, 29.

bu sistemde; bilişim ağları ve iletişim araçları yoluyla verilerin aktarılması söz konusudur.[10]

5237 sayılı TCK'nin 243. maddesinde düzenlenen bilişim sistemine girmek ve orada kalmaya devam etmek suçu, 765 sayılı TCK'nin525-a /1 ve 525- a /2'de yer alan "verilerin ele geçirilmesi" ve "ele geçirilen verilerin zarar vermek üzere kullanılmaları" suçlarının karşılığı olarak görülse de bu suçları düzenlememektedir.[11] 765 sayılı mülga TCK' da bilişim sisteminden birtakım verilerin ele geçirilmesi cezai yaptırıma bağlanmıştır. Buna karşılık bilişim sistemindeki verilerin ele geçirilmesi amacına yönelik olmaksızın, sadece sisteme girip orada kalmayı cezalandıran bir hüküm bulunmamaktaydı.[12] Bu bağlamda 5237 sayılı TCK'nin243. maddesindeki düzenleme ile sözgelimi bir başkasının sosyal medya hesabına gizlice girip sistemde kalmaya yönelik bu tür fiillere, ilk kez cezai yaptırım uygulanmış ve böylece mevzuattaki eksiklik giderilmiştir.[13]

5237 sayılı Türk Ceza Kanunu'nda 765 sayılı eski Türk Ceza Kanunu'ndan farklı olarak bilişim sistemlerinden söz edilmiştir. Bu düzenlemede; bilişim suçlarının genel olarak bir sisteme izinsiz olarak girilmesi sonucu ortaya çıktığı görülmektedir. Anılan maddenin gerekçesinde bilişim sistemleri, *"verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemler*" olarak tanımlanmaktadır.[14] Buna bağlı olarak bilişim teknolojisinin sürekli olarak değişimi ve yeniliği nedeni ile birden fazla sistem aracılığıyla da bu suç işlenebilir. Burada sistemlerden kastedilen ise mekanik, elektronik ve manyetik araçlardır. Dolayısıyla salt bilgisayar, cep telefonu ve internet akla gelmemelidir. Bu konuda birbirlerine

[10] Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Hukukunda)," *Gazi Üniversitesi Hukuk Fakültesi Dergisi 14,* no. 2, (2010): 285.

[11] Levent Kurt, Açıklamalı *İçtihatlı Tüm Yönleriyle Bilişim Suçları*, (Ankara: Seçkin Yayınevi, 2005), 53.

[12] Kurt, *Bilişim Suçları*, 54.

[13] Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*, 204.

[14] Erdağ, "Bilişim," 289.

bilişim ağı üzerinden bağlanabilen her türlü sistem, bilişim sistemi şeklinde değerlendirilebilir.[15]

Bilişim sistemine hukuka aykırı olarak erişim, diğer suçların işlenmesine de olanak tanıyacağı için fiilin ayrıca cezalandırılması gerekmektedir. Dolayısıyla bilişim sistemine girme suçu, TCK'nin m. 244 ve m. 245 hükümlerinde doğrudan bilişim suçları içerisinde yer almaktadır. Bilişim sistemlerinin araç olarak kullanılması yoluyla işlenen suçlar ise genel olarak o suçla ilgili maddede düzenlenmiştir. Sözgelimi, TCK'nin 142. maddesinin 2. fıkrasının e bendinde yer alan "*nitelikli hırsızlık*"ile TCK'nin 158. maddesinin 1. fıkrasının f bendinde yer alan "*nitelikli dolandırıcılık*" suçları bu duruma örnek olarak gösterilebilir.[16]

Yargı Reformu Strateji Belgesi'nde yer alan İnsan Hakları Eylem Planı'nda *"Makul Sürede Yargılanma Hakkının Güçlendirilmesi"* başlığı altında; *"Bilişim alanında işlenen suçlar ile dolandırıcılık suçları başta olmak üzere soruşturma aşamasında ortaya çıkan yetki uyuşmazlıklarının hızlı bir şekilde sonuçlandırılması amacıyla gerekli tedbirler alınacaktır."* denilerek, bilişim suçları kaynaklı uyuşmazlıkların hızlı bir şekilde sonuçlanması için gereken tedbirlerin alınacağı ifade edilmiştir.[17] 30.11. 2021 tarihinde Resmi Gazete'de yayımlanan HSK kararı ile ihtisas mahkemelerine "bilişim ihtisas mahkemeleri" eklenmiştir Böylece bilişim suçlarına ilişkin olarak uyuşmazlıklar, münhasıran bu suçlara yönelecek ihtisas mahkemeleri sayesinde daha hızlı ve makul bir şekilde çözüme kavuşturulacaktır. Çalışmamızda "*bilişim sistemleri girme ve kalma*" suçlarına yönelik genel açıklamaların ardından korunan hukuki yarar konusunu ele alacağız.

[15] Durmuş Tezcan, Mustafa Ruhan Erdem ve Murat Rifat Önok, *Teorik ve Pratik Ceza Özel Hukuku,* 17. Baskı (Ankara: Seçkin Yayıncılık 2019), 1116.

[16] Erdağ, "Bilişim," 289.

[17] Nagihan Merve Akaslan, "Yeni Bir İhtisas Mahkemesi Olarak Bilişim Mahkemesi," https://www.Hukukihaber.Net/Yeni-Bir-İhtisas-Mahkemesi-Olarak-Bilisim-MahkemesiMakale,8797.Htm Erişim tarihi: 31 05.2021.

II. KORUNAN HUKUKSAL YARAR

Bilişim sistemine hukuka aykırı olarak girme ya da bilişim sisteminde kalmaya devam etme suçunda korunan hukuki yararın birden fazla yönü bulunmaktadır.[18] Bilişim alanında TCK'nin uygulama alanına giren bilişim sistemini engelleme, bozma ve yer değiştirme suçu (TCK. m. 244) banka veya kredi kartlarının kötüye kullanılması (TCK m.245) suçunun işlenmesi için bilişim sistemlerine girilmesi gerekmektedir. Dolayısıyla bu düzenlemenin yapılmasındaki temel amaç, sisteme girişin engellenmesidir. Bilişim sistemine girme ya da orada kalmaya devam etme suçu ile korunan başlıca yarar, kamu düzeninin korunmasıdır.[19] Buna bağlı olarak kişisel verilerin ve özel hayatın gizliliğinin korunması ve haberleşmenin gizliliğinin sağlanması amaçlanmaktadır. Böylelikle bilişim sistemini kullanan kimselerin hakları korunacağı gibi diğer bilişim yoluyla işlenen suçların engellenmesi de mümkün olacaktır.[20]

Anayasamızın 21. maddesinde düzenlenen konut dokunulmazlığı ilkesi gereği *"usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin konutuna girilemeyeceği, arama yapılamayacağı ve buradaki eşyaya el konulamayacağı* hüküm altına alınmıştır. Anılan düzenlemeden anlaşılacağı gibi nasıl ki kimsenin özel mülküne usulüne uygun yetkili mercii kararı bulunmadıkça keyfi olarak girilemiyor ise hiç kimsenin de bilişim sistemlerine de izinsiz olarak girilmesi mümkün değildir.[21] Aksi takdirde bilişim sisteminin dokunulmazlığının ihlali söz konusu olacaktır. İşte; bilişim sistemlerine yönelik bu tür müdahalelerin artması, sistemlerin yetkisiz müdahalelerden korunmasını gerekli kılmaktadır.

[18] A. Caner Yenidünya, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu," *Legal Fikri ve Sınai Haklar Dergisi* 4, (2005), 1023.

[19] Kurt, *Bilişim Suçları*, 64.

[20] Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*, 166.

[21] Olcay Suphan, "Konut Dokunulmazlığı Hakkı ve Konut Dokunulmazlığının İhlali Suçu," *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 6,* no. 1, (Bahar 2019): 234.

Bu nedenle bilişim sistemine yetkisiz olarak girilmesi ya da orada kalmaya devam edilmesi fiilleri, suç kapsamına sokularak cezalandırılmaktadır.[22]

Günümüzde teknolojik gelişmelerin sürekli ivme kazanması sonucu, internetin ve elektronik araçların, iletişimde öncü bir rol üstlendiği görülmektedir. Doktrindeki bir görüşe göre bu suçla korunan hukuki yararın öncelikle bilişim sisteminin güvenliği olduğu, bu sayede kişilerin verilerinin korunmasının yanı sıra özel hayatın dokunulmazlığı gibi kişisel menfaatlerin de korunduğu ifade edilmektedir. Bu düzenlemenin çıkarılmasındaki temel etkenin, bilişim sisteminin güvenliği ve dokunulmazlığı olduğu belirtilmiştir.[23] Bu bağlamda bilgisayar ve mobil cihazların belleğinde bulunan kişisel verilerin korunması, özel hayatın gizliliği açısından da hayati önem taşımaktadır. Yukarıda zikredilen konut dokunulmazlığının korunmasında olduğu gibi Anayasamızın 20'nci maddesinde düzenlenen özel hayatın *gizliliği*" ve Anayasamızın 22. maddesinde yer alan "*haberleşme hürriyeti"* de bilişim sistemlerinin kullanımı yönünden fevkalade önem taşımaktadır. Modern dünyada; haberleşmenin ve iletişimin, mobil araçlar ile sağlanması, bu araçların bağlantılarındaki gizliliğinin korunması sorununu gündeme getirmiştir. Bu noktada; bir kişinin bilgisayarı ya da cep telefonundaki verilerin, sistem sahibinin rızası olmadan üçüncü kişiler tarafından kullanılmaması hem haberleşme özgürlüğü hem de özel hayatın gizliliği hakkı yönünden önemlidir. Aksi takdirde bilişim sistemine yetkisiz kişilerin erişmesi ve bu sistem üzerinde egemenlik kurması, sistem sahipleri ile kullanıcıların, mağduriyetine neden olacaktır. Bu nedenle; bilişim sistemine girme ya da orada kalma suçu, diğer suçların işlenmesine de zemin hazırlamaktadır.[24] Sözgelimi, yetkin olmayan bir kişinin, başkasına ait sosyal medya hesap şifresini izinsiz olarak kullanması da haberleşme özgürlüğü ve özel hayatın gizliliği haklarının ihlaline yol açabilir.[25]

[22] Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 12,* (*Özel Sayı* 2012): 1364.

[23] Erdoğan, "Bilişim," 1365.

[24] Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, (Ankara: Adalet Yayınevi, 2008), 79.

[25] Taşkın Şaban Cankat, "Bilişim Hukuku Uluslararası Uyuşmazlıklar," *Türkiye Barolar Birliği Dergisi* 85, (2009): 336.

Bu konuya ilişkin Yargıtay bir kararında; "Sanığın savunmasında, katılanla evli olduğu dönemde mail adreslerinin şifrelerini bilmesi nedeniyle mail adreslerine girdiğini, mail adreslerinin şifrelerini kırmadığı ve değiştirmediğini beyan ettiği, sanığın kullandığı bilgisayar üzerinde yapılan inceleme sonrası düzenlenen bilirkişi raporlarında da, sanığın, katılana ait mail adreslerine girdiğinin tespit edildiği, ancak üçüncü kişilerle yazışma yaptığına dair kayıtlara rastlanmadığının bildirildiği dikkate alındığında, sanığın aksi kanıtlanamayan savunmaları ve tüm dosya kapsamı birlikte değerlendirildiğinde, sanığın, katılana ait iki farklı mail adreslerine izinsiz olarak girme eyleminin TCK'nin 243/1.maddesinde düzenlenen bilişim sistemine girme suçunu" oluşturduğu belirtilmiştir.[26] Görüldüğü gibi yetkin olmayan bir kişinin, başkasına ait sosyal medya hesap şifresini izinsiz olarak kullanması da haberleşme özgürlüğü ve özel hayatın gizliliği haklarının ihlaline yol açmıştır.

Türk Ceza Kanunu'nun 243. maddesine son fıkrasına 24.03.2016 tarihinde 6698 sayılı kanunun 30. maddesinde yapılan değişiklikle; bilişim sisteminin tamamına veya bir kısmına hukuka aykırı olarak girmek veya orada kalmaya devam etme, suç olarak kabul edilmektedir. Böylelikle suçun işlenebilmesi için bilişim sisteminin tamamına ya da bir kısmına girilmesi veya orada kalmaya devam edilmesi seçimlik hareketleri aranmış ve böylelikle; bilişim sistemlerinin korunması sağlanmak istenmiştir. Bu düzenleme öncesinde, bir fiilin suç teşkil etmesi için hem bilişim sistemine girme hem de orada kalmaya devam etme fiillerinin bir arada bulunması koşulu arandığı için hükmün uygulanması konusunda doktrinde birtakım tartışmalar yaşanmıştır.[27] Doktrinde suçun, kullanıcıların, internet ortamında üçüncü kişilerin haksız erişimi ile rahatsız edilmemesi ve kişisel hakların korunması amacıyla düzenlendiği yönünde görüşler bulunmakla birlikte TCK'nin 243. maddenin 2. fıkrasında fiil yönünden daha az cezayı gerektiren halin düzenlenmiş olması, bu hükmün, bilişim sisteminin korunması amacı ile çıkarılmadığı görüşünü de desteklemektedir.[28] Buna bağlı olarak bilişim sistemine girme suçu ya da orada kalma suçu ile kişilerin dijital ortamdaki özel alanının korunması amaçlanmaktadır. Madde gerekçesine bakıldığında;

[26] Yargıtay 12. CD, E. 2015/9555, K. 2016/10731, K.T. 22.06.2016.

[27] Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*, 202.

[28] Karakehya, "Türk," 17.

hangi hukuki yararın gözetildiğine bakılmaksızın, korunmak istenen temel amacın, internet ortamındaki kişisel alan olduğu sonucuna varılabilir.[29]

Doktrinde baskın görüş ise, bu suçlarla ilgili korunan hukuki yararın, bilişim sisteminin güvenliği ve özel hayatın gizliliği gibi alanlarla sınırlı kalmadığını, bu kavramı da aşan nitelikte kamu düzeninin korunması olduğunu zikretmektedir. Bunun sonucu olarak eğitim, iletişim, hukuk gibi konularda kamu düzenini ve güvenliğini tehdit eden bu suçlarda, kamu düzeninin korunması fevkalade önem taşımaktadır.[30] Kanaatimizce bilişim sistemine girme ve kalma suçlarının, TCK'da "Topluma Karşı Suçlar" başlığı altında düzenlenmesi nedeni ile korunan hukuki yararın, kamu düzeninin korunması olduğunu ifade edebiliriz.

III. FAİL

5237 sayılı TCK'nin 243. maddesinde suçta cezalandırılacak kişi için *'kimse'* ibaresinin kullanıldığı görülmektedir. Anılan hükümden, bu suçun failinin herkes olabileceği sonucuna ulaşılmaktadır. Bunun sonucu olarak bilişim sistemine yetkisi olmadığı halde hukuka aykırı olarak giren veya orada kalmaya devam eden herkes bu suçun faili olabilir. Dolayısıyla bu suçun işlenmesi için üst düzey bir bilişim sistemi programcısı donanımına sahip olma şartı aranmamaktadır; orta zekaya sahip mobil cihaz veya bilgisayar kullanma becerisine sahip kişiler de bu suçun faili olabilir.[31] Bu nedenle bilişim sistemlerine yönelik işlenen suçun failleri genel olarak bilişim korsanı, hacker, kod kıran kişi veya *craker* olarak da tanımlanmaktadır.[32]

Bilişim sistemine girme suçunun failinin belirlenmesinde IP numarasını kullanan kişi her zaman suçun doğrudan faili olmamaktadır, Buna bağlı olarak IP numarasının kayıtlı olduğu kişi, suçun faili olabileceği gibi başka bir kimse de suçun faili olabilir. Bu nedenle ceza yargılamasında, failin belirlenmesi amacı ile objektif sorumluluk esasından farklı bir durum

[29] Cengiz Apaydın, *Bilişim Suçları ve Bilişim Ceza Hukuku*, (İstanbul: Acar Matbaacılık, 2017), 51.

[30] Apaydın, *Bilişim Suçları ve Bilişim Ceza Hukuku*, 52.

[31] Yenidünya ve Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, 57.

[32] Erdoğan, "Bilişim," 1392.

ortaya çıkmaktadır. Çünkü, IP numarasını kullanarak bilişim sistemine girme suçunu işlediği iddia edilen kişiye yönelik ceza soruşturmasında; maddi gerçeğin belirlenmesi amaçlanmaktadır. Bu nedenle IP numarası, diğer deliller ile desteklenmek kaydı ile kullanılabilir. Dolayısıyla bu durum, objektif sorumluluktan ayrı olarak düşünülmelidir.[33]

Yargıtay konuya ilişkin bir kararında;

> "….sanığın, şikayetçinin kullandığı ".....@hotmail. com" e-posta adresi ile irtibatlı olan ... adresine bilgisi ve rızası olmaksızın şifreyi değiştirerek erişilmez kıldığından bahisle açılan davada, yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan hüküm kurulmuştur. Sanığın suçlamayı kabul etmediği gibi hattına başkalarının girmiş olabileceği savunmasına ilişkin olmak üzere internet hattını sanık dışında başkalarının da kullanıp kullanmadığı ve kendisine ait olduğu belirtilen e-mail adresinin sanığa aidiyeti hususunda dosyada bir bilgiye rastlanmamıştır. Şikayetçinin bir aydır e-mail adresine giremediğini belirttiğinin anlaşılması karşısında, anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit edilmemiştir. Sanık tarafından suç tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulması gerektiği gözetilmeden eksik inceleme ile hüküm kurulması"[34]

denilerek bilişim sistemine girme suçunun oluşması için gerekli tüm tespitlerin yapılmasının zorunlu olduğu, somut olayın niteliğine göre hangi IP numarası ile erişim sağlandığı belirlenmeden dosya üzerinden karar verilemeyeceği ortaya konulmuştur.

Ankara Bölge Adliye Mahkemesi'nin bir kararında da "Sanık hakkında TCK'nin 243. maddesi gereğince bilişim sistemine girme suçundan cezalandırılması istemi ile açılan kamu davasında;

[33] Apaydın, *Bilişim Suçları ve Bilişim Ceza Hukuku*, 53.

[34] Yargıtay 8. CD, E. 2018/1078, K. 2018/2485, K.T. 08.03.2018.

> "…A.Ş kayıtlarında sanığın Bayram'ın babası Osman'ın IP numarasının tespit edildiği, sanığın babasının bilgisayarın oğlu Bayram tarafından kullanıldığını beyan ettiği, sanığın atılı suçu işlediği yönünde aşamalarda hiç bir ikrarının bulunmadığı, IP adresinin iddianamede delil olarak gösterildiği ancak IP adresinin kişiye özel olmadığı, IP'nin teknik açıdan değiştirilebilir yapıda olduğu, başka bir kişinin de mevcut IP adresini kullanabileceği, sistem havuzunda IP adresinden çıkıldıktan sonra başkasının da IP'yi kullanabileceği, internet üzerinden alışverişin herhangi bir kişi tarafından da yapılabileceği, abonelik üzerinden başkalarının da bağlanmış olabileceği göz önüne alınarak bu hususların açıklığa kavuşturulması amacıyla bilirkişi raporu alınmaksızın eksik inceleme ile yazılı şekilde karar verilmesi"[35]

bozma nedeni olarak yer almaktadır. Bu kararda da IP adresinin değiştirilebilir nitelikte olduğu ve birçok kişi tarafından kullanılabileceği vurgulanmış; ayrıca failin belirlenmesinde teknik incelemenin tereddüte yer bırakmayacak şekilde yapılması gerektiğine dikkat çekilmiştir.

Yargıtay'ın konuya yönelik içtihatlarında, temel yaklaşım, şu şekilde özetlenebilir:

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

[35] Ankara BAM 13. CD, E. 2018/3653, K. 2019/1533; Uğur İhtiyaroğlu**,** "Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi", *Hacettepe Üniversitesi Hukuk Fakültesi Dergisi,* (2020): 411.

sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır.[36]

Yargıtay'ın konuya ilişkin kararında,

"….Dosya kapsamından, katılana ait mail adreslerine, sanıklara ait şirketler tarafından kullanılan IP adreslerinin erişim sağladığının sabit olduğu, bunun yanında bilgisayar ve yazılım şirketinin sorumlusu olan sanık ...'ın savunmalarında, 77.79.83.186 IP numaralı sunucularına suç tarihinde 65.200.157.177 numaralı IP ile sürekli atak yapıldığını belirttiği, diğer sanık ...'in de atılı suçu işlemediğini beyan ettiği, suçların 2009 tarihinde işlenmesi nedeniyle sanıklara ait bilgisayarlarda yapılması gerekli olan ama yapılmayan incelemelerin, aradan geçen zaman itibariyle şimdi yapılması halinde bir delile ulaşılması mümkün görülmemekte ise de; dosyanın kül halinde bilişim alanında uzman bilirkişiye tevdi edilerek, 24/12/2009 günü saat 23.00 ile 25/12/2009 günü saat 09.00 tarihleri arasında, katılana ait mail adreslerine sanıklar dışında başka IP adreslerinin ulaşıp ulaşmadığı, sanıklara ait IP numaraları vasıtasıyla, başka IP numaraları ile uzaktan atak yapılarak katılana ait mail adreslerine erişilip erişilemeyeceği konularında, katılanın iddiası ve sanıkların savunmaları dikkate alınarak ayrıntılı bilirkişi raporu alınması, ayrıca katılanın şikayet dilekçesinde bahse konu mail adreslerindeki kayıtların internet ortamında yayınlanmış olduğunu ve başka postalara kendisi adına mail adresi göndermiş olduğu iddiası da gözetilerek, bu kayıtların hangi internet sitelerinde yayınlandığı, bu yayınlara ilişkin çıktıların bulunup bulunmadığı, kendisine ait mail adresinden üçüncü kişilere gönderildiği belirtilen mail çıktılarının bulunup bulunmadığı, üçüncü kişilerin kimlik bilgileri tespit edilerek, gerektiği takdirde tanık sıfatıyla dinlenmesi sağlandıktan sonra sanıkların hukuki durumunun tayin ve takdiri gerekirken, eksik incelemeyle yazılı şekilde hüküm kurulması"[37]

kanaatine ulaşmıştır.

Yargıtay'ın bir başka bir kararında ise;

[36] İhtiyaroğlu, "Bilişim," 433; Yargıtay 8. CD, E. 2018/1078, K. 2018/2485, K.T. 08.03.2018.

[37] Yargıtay 12. CD, E. 2015/7248, K. 2016/6819, K.T. 20.04.2016.

> "…sanık tarafından suç tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulması gerektiği gözetilmeden eksik inceleme ile hüküm kurulması"[38]

bozma nedeni olarak kabul edilmiştir. Bu kararlarda, fail tarafından gerçekleştirilen bilişim sistemine girme eyleminin şüpheye yer bırakmayacak şekilde araştırılması gerektiği, özellikle IP numarası üzerinde kuşkuya yer vermeyecek şekilde inceleme yapılarak sonucuna göre karar verilmesi gerektiğinin altı çizilmektedir.

IV. MAĞDUR

Suçun mağduru, bilişim sistemine girilmesi ya da bu sistemde kalmaya devam edilmesi nedeni ile kişisel hakları tehlikeye düşen herkes olabilir.[39] Doktrinde baskın görüş, normatif düzenlemelerde Türk Ceza Hukuku sisteminde mağdurun ancak gerçek kişi olabileceğini kabul etmektedir.[40] Buna karşılık doktrinde suçun mağdurunun gerçek kişiler dışında, tüzel kişiler de olabileceği ileri sürülmektedir. Daha önce de belirttiğimiz gibi suçla korunmak istenen bilişim sisteminin güvenliğini tedarik etmektir. Bu nedenle gerçek kişiler dışında tüzel kişiliği haiz bilişim sistemlerinin sahipleri de mağdur konuma düşebilir.[41] Buna karşılık tüzel kişilerin bu suçtan ötürü sadece *"zarar gören"* olabileceği tezini savunanlar, doktrinde çoğunlukta bulunmaktadır.[42] Doktrinde azınlıkta kalan görüş ise tüzel kişilerin de bu suçun mağduru olabileceği yönündedir. Buna gerekçe olarak da bilişim sistemi üzerinde hak sahibi olan bir şirketin hesaplarının hackerler tarafından ele geçirilmesi ya da izinsiz olarak tüzel kişiliğe ait gizli bilgilere erişilmesi örnek olarak gösterilebilir. Burada; tüzel kişilerin de bilişim sistemi

[38] Yargıtay 8. CD, E. 2018/1078 K. 2018/2485.

[39] Tezcan, Erdem ve Önok, *Teorik ve Pratik Ceza Özel Hukuku,* 1149.

[40] İhtiyaroğlu, "Bilişim," 434.

[41] Erdoğan, "Bilişim," 1394.

[42] Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi," *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 71,* no. 1, (2013): 858.

ve/veya veriler üzerinde mülkiyet hakkı, kira ve vedia gibi sözleşmelerden kaynaklanan tasarruf hakkı bulunduğu ileri sürülmektedir.[43]

Tüzel kişilerin de suçun mağduru olabileceğine yönelik olarak Yargıtay bir kararında;

> "…Şikayetçi şirketin sistemine hukuka aykırı olarak girerek, sistemin işleyişini engelleme, bozma, sistemdeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme şeklindeki TCK'nin 244/1-3.madde ve fıkralarında yazılı hallerin gerçekleşmemesi nedeniyle, anılan maddenin 4. fıkrasının uygulanamayacağı, şikayetçi şirkete ait sisteme hukuka aykırı olarak girme ve orada kalmaya devam etme şeklindeki eylemin TCK'nin 243/1. madde ve fıkrasında düzenlenen suçu oluşturacağının gözetilmemesi, bozmayı gerektirmiştir."[44]

şeklindedir.

V. MADDİ UNSUR

Bilişim sistemine girme veya bilişim sisteminde kalma suçunda maddi unsurları maddi konu, fiil, netice ve nedensellik bağı hususlarında irdelemelerimizin ardından nitelikli haller, hukuka aykırılık ve manevi unsur konularına da yer vereceğiz.

A) SUÇUN KONUSU: BİLİŞİM SİSTEMLERİ

Günümüzde haberleşme ve bilişim teknolojilerinde yaşanan baş döndürücü değişim ve ilerleme, anında veri alma ve iletme olanağı sağlamaktadır. Bunun dışında bilgisayar, mobil cihazlar ve diğer elektronik araçlar kanalı ile sesli, yazılı ve görüntülü içerikler de paylaşılmakta; kablosuz teknolojinin giderek arttığı görülmektedir.[45] Buna bağlı olarak bilişim teknolojisindeki değişimin etkisi ile geçmişle kıyaslanmayacak oranda kullanıcı sayısının hızla arttığı gözlemlenmektedir. Mülga 765 sayılı Türk Ceza Kanunu'nda

[43] Kurt, *Bilişim Suçları*, 163.

[44] Yargıtay 11. Ceza Dairesi E. 2012/439, K. 2013/16403, K.T. 11.11.2013.

[45] Fahri Atasoy, "Kültürler Üzerinde Bilişim Devriminin Etkileri," *Modern Türklük Araştırmaları Dergisi 4,* no. 2, (2007): 168.

"bilgileri otomatik olarak işleme tabi tutmuş sistem" ifadesi kullanılmıştı. 5237 sayılı Türk Ceza Kanunu'nda ise bu ifade yerine "bilişim sistemi" terimi kullanılmıştır.[46]

5237 sayılı Türk Ceza Kanunu yönünden değerlendirildiğinde bir sistemin bilişim sistemi olup olmadığı, somut olayın özelliğine göre konusunda uzmanlaşmış kişiler tarafından yapılacak teknik bir inceleme sonucu belirlenmelidir.[47] Bilişim sistemi, bilgisayar ve internet ile doğrudan bağlantılıdır. Buna etken olarak da son çeyrek asırda internetin dünya genelinde kullanımının yaygınlaşması ile bilişim sistemlerinde, küresel düzlemde iletişim ağı kurulması gösterilebilir. Dolayısıyla bu sistem üzerinde bilgisayarların ortak bir alanda birbirlerine bağlanması sonucu elektronik ağ (*network*) oluşmuştur. Buna bağlı olarak da dünyanın farklı bölgelerindeki insanların mobil cihazlar ya da bilgisayarları aracılığı ile sisteme entegre olması sonucu çevrimiçi olarak bilgi alışverişinde bulunulmaktadır.[48] Bununla birlikte bilgisayar dışında da veriler arasında bağlantı sağlayabilen elektronik ve manyetik cihazlar aracılığı ile veri akışı sağlanabilir. Bu durumda; bilişim sistemlerine girme ya da orada kalma suçu, internet ağı kullanılmaksızın manuel olarak da işlenebilir.[49]

Yargıtay Ceza Genel Kurulu'nun bir kararında;

> "Elektronik beyin" veya "bilgileri otomatik işleme tabi tutmuş sistem" olarak adlandırılan bilgisayar; "çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran, bilgileri depolayan elektronik araç, elektronik beyin" anlamına gelmektedir. İnternet ise, dünya üzerindeki milyonlarca bilgisayarın birbirlerine bağlanmaları ile oluşan global

[46] Hüseyin Koçak ve Ali Nazmi Dandin, "Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri," *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi 19*, no. 1, (2017): 139.

[47] Özge Apiş, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri," *Yasama Dergisi* 37, (2018): 49.

[48] Ömer Tekelli, "Bilişim Suçlarıyla Mücadelede Polisin Yeri*" Sayder Dış Denetim Dergisi*, (Temmuz-Ağustos-Eylül 2011): 83.

[49] Richard W. Boss, *Intranet and Extranet* PLA Technotes, American Library Association, 2010, 2.

> bir bilgisayar ağları sistemi olarak nitelendirilmiştir. Bilişim ise "insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi"[50]

şeklinde tanımlanmıştır.

5237 sayılı Türk Ceza Kanunu'nun 243. maddesinde düzenlenen bilişim sistemine girme suçu ya da orada kalma suçunun konusunu, yukarıda da izah ettiğimiz "*bilişim sistemi"* oluşturmaktadır. Bilişim sistemi kavramı, TCK'nin 243. maddesinin gerekçesinde, *"verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tutma olanağı veren manyetik sistemler"* şeklinde açıklanmıştır.[51] Ayrıca ülkemizin de taraf olduğu Avrupa Konseyi Siber Suçlar Sözleşmesinin 1. maddesinde "*bilgisayar sistemi, bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder"* şeklinde tanımlanmıştır.[52] 5237 sayılı TCK'nin 243. maddesi uyarınca bu suçun işlenebilmesi için bilişim sistemine hukuka aykırı olarak girilmesi ya da orada kalmaya devam edilmesi gerekmektedir. Buna bağlı olarak bilişim sistemine yetkili olmadığı halde izinsiz olarak giren kimseler, "*bilgisayar korsanı"* ya da *"hacker"* olarak nitelendirilmektedir.[53]

TCK'nin 243. maddesi uyarınca, bilişim sistemine girme suçunun oluşabilmesi için bilişim sisteminin tamamına ya da bir kısmına hukuka aykırı olarak girilmesi gerekmektedir. Bunun dışında bilişim sistemine rızaen girilmekle birlikte içerisinde hukuka aykırı şekilde kalınan bilişim sistemi de bu suçun konusunu oluşturmaktadır. Anılan maddenin ikinci fıkrası yönünden suçun konusunu *"bedeli karşılığında yararlanılabilen bilişim sistemleri"* oluşturmaktadır. Şayet bu suç, *"Otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmet"* karşılığında işlenir

[50] Yargıtay Ceza Genel Kurulu, E. 2016/23-1033 K. 2020/2 sayılı kararı aktaran İhtiyaroğlu, "Bilişim," 418.

[51] Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* 4. Basım, (Ankara: Adalet Yayınevi, 2017), 810.

[52] Yenidünya ve Değirmenci, *Bilişim Suçları*, 27.

[53] Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*, 169.

ise TCK'nin 163. maddesinde düzenlenen "*Karşılıksız Yararlanma"* kapsamına girecektir.[54] Dolayısıyla TCK'nin 243. maddesinin ikinci fıkrası kapsamına girmesi için fail tarafından bedeli ödenmek suretiyle girilebilecek bir sisteme, bedel ödenmeden girilmesi veya orada kalınması gereklidir. Bu noktada, bedel karşılığı yararlanılabilen bilişim sistemlerinin neler olduğu konusu madde gerekçesinde açıklanmasa da web siteleri, şifreli televizyon ve kiralama karşılığı yararlanılabilen bilişim sistemleri, cep telefonları ve diğer elektronik cihazlara anlaşma karşılığı gönderilen reklam mesajları ve mailler, internet servis sağlayıcı hizmetlerinden yararlanılması uygulamaları anlaşılmaktadır.[55]

Yargıtay 11. Ceza Dairesi'nin bir kararında;

> "… sanık (M.İ.) (D.)'e abone olmuş ve bunun karşılığında (D.)'ten kendisine verilen kullanıcı bilgilerini, CardSharing yöntemi ve (D*) uydu alıcısı aracılığıyla başka kişilerle para karşılığında paylaştığı mevcut olan deliller ışığında tespit edilmiştir, hususlarının ifade edilmesi karşısında, her ne kadar katılan tarafça verilen şifreler üzerinde oynama yapılmadığı belirtilmiş ise de, sanığın katılan firmanın şifreleme sistemine herhangi bir müdahalede bulunup bulunmadığı, yayınların şifresiz olarak izlenebilmesini sağlamak için sisteme veri yerleştirip yerleştirmediği, sistemdeki verileri bozup bozmadığı, keza sistemdeki verileri değiştirmek veya bir yerden başka bir yere göndermek şeklinde bir eylem gerçekleştirip gerçekleştirmediği hususlarının tam olarak belirlenmesi bakımından hükme esas alınan bilirkişi kurulu raporunun yeterli ve açıklayıcı nitelikte bulunmadığı, sanığın, sistemle bağlantıyı tam olarak nasıl sağladığı, ne gibi aşamalardan geçirilerek şifreli yayının izleyiciye şifresiz olarak izlettirildiği konusunda tatmin edici ve hükme esas alınabilecek nitelikte tespitlerin yapılmadığı görülmekle, bir teknik üniversiteden seçilecek konusunda uzman 3 kişilik bilirkişi kuruluna dosyanın ve emanet muhteviyatı eşyaların kül halinde tevdiine…"[56]

[54] Zahit Yılmaz ve Özge Apiş, "Karşılıksız Yararlanma Suçu (TCK m.163)," *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 19,* no. 2, (2013): 1759. Erdoğan, "Bilişim," 1396-1399.

[55] Erdoğan, "Bilişim,"1396-1399.

[56] Yargıtay 11. Ceza Dairesi E. 2012/439 K. 2013/16403 K.T. 11.11.2013.

ifadesine yer verilerek şifreli bir yayının izlenmesi sonucu TCK'nin 243. maddesi uyarınca bilişim sistemine hukuka aykırı olarak girme suçunun unsurlarının oluşup oluşmadığının bilirkişi raporu sonucu belirlenebileceği kanısına varmıştır.

TCK'nin 243. maddesinin 3. fıkrasında suçun, neticesi sebebiyle ağırlaşmış halini düzenlemiştir.[57] Anılan hüküm uyarınca, *"bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunacağı* belirtilmiştir.[58] Böylece verilerin yok olması veya değiştirilmesi ile bilişim sistemine girme suçunun, neticesi sebebiyle ağırlaşmış hali gerçekleşmektedir.[59] Bunun sonucu olarak bilişim sistemine hukuka aykırı olarak girilmesi ya da bilişim sisteminde kalmaya devam edilmesi sonucunda "*sistemin içerdiği veriler yok olur ya da değişirse"* cezayı arttırıcı bir etken olacaktır.

Anılan hüküm uyarınca failin kastı, bilişim sistemine hukuka aykırı girme ya da orada kalmaya yönelik olmalıdır. Aksi takdirde sistemdeki verileri yok etme ya da değiştirmeye yönelik bir kastı bulunduğu takdirde bu hükmün uygulanması mümkün değildir. Buna karşılık failin bu yönde bir kastı olmasa dahi bilişim sistemine hukuka aykırı girmesi sonucu veriler yok olur ya da değişirse, failin ağırlatıcı nedenden sorumlu tutulabilmesi için en azından taksirli bir hareketinin bulunması gerekir.[60]

Failin kastı, bir bilişim sistemindeki verileri bozma, yok etme değiştirme ya da erişilmez kılma gibi hareketlerden oluşuyor ise TCK'nin 244. maddesinin 2. fıkrası gereği sorumlu tutulacaktır. Görüldüğü gibi TCK'nin 244. maddesinde yer alan *"Sistemi Engelleme, Bozma, Verileri Yok Etme ya*

[57] İsmail Malkoç, *Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu II*, (Ankara: Malkoç Kitabevi, 2007), 1671.

[58] 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* 62, (2006): 123.

[59] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız ve İlker Tepe, *Türk Ceza Hukuku Özel Hükümler*, 11. Basım, (Ankara: 2017, Seçkin Yayıncılık), 951.

[60] Yılmaz Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi," *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 2,* no. 2, (2005): 404.

da Değiştirme" suçundan farklı olarak failin sisteme hukuka aykırı olarak girmesi ya da orada kalması durumunda sistemdeki veriler yok olmakta ya da değişmektedir.[61]

Failin hukuka aykırı olarak bilişim sistemine girme veya orada kalma kastının bulunmaması durumunda suçun temel şekli meydana gelmeyeceğinden failin sorumluluğu doğmayacaktır. Bu halde TCK'nin 243. maddesinin 3. fıkrası oluşmayacağı gibi ancak kasten işlenebilen TCK'nin 244. maddesinin 2. fıkrasının uygulanması söz konusu olamaz.[62] TCK'nin 243. maddesinin 4. fıkrası yönünden ise suçun konusunu "Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakilleri" oluşturmaktadır.

Yargıtay 12. Ceza Dairesi'nin 22.06.2016 tarihli bir kararında;

> "Sanığın savunmasında, katılanla evli olduğu dönemde mail adreslerinin şifrelerini bilmesi nedeniyle mail adreslerine girdiğini, mail adreslerinin şifrelerini kırmadığı ve değiştirmediğini beyan ettiği, sanığın kullandığı bilgisayar üzerinde yapılan inceleme sonrası düzenlenen bilirkişi raporlarında da, sanığın, katılana ait mail adreslerine girdiğinin tespit edildiği, ancak üçüncü kişilerle yazışma yaptığına dair kayıtlara rastlanmadığının bildirildiği dikkate alındığında, sanığın, katılana ait iki farklı mail adreslerine izinsiz olarak girme eyleminin sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu değil, TCK'nin 243/1.maddesinde düzenlenen bilişim sistemine girme suçunu oluşturur."[63]

Yargıtay 9. Ceza Dairesi'nin 07.04.2014 tarihli bir kararında ise;

> "Katılan E.T.'ye ait MSN adresine şifresini kırmak suretiyle hukuka aykırı olarak giren ve orada kalmaya devam eden sanığın eyleminde, 5237 sayılı Yasa'nın 243/1. madde ve fıkrasında yer alan suçun yasal unsurlarının oluştuğu gözetilmeden, sanığın mahkumiyeti yerine yazılı biçimde beraatine karar verilmesi…"[64]

denilerek mail şifresinin kırılması suretiyle girilmesi "bilişim sistemine girme" suçunu oluşturacağı ifade edilmiştir.

[61] Eker, "Türk,"125.

[62] Apaydın, *Bilişim Suçları ve Bilişim Ceza Hukuku*, 71.

[63] Yargıtay 12. CD, E. 2015/9555, K. 2016/10731, K.T. 22.06.2016.

[64] Yargıtay 9. CD, E. 2013/3214, K. 2014/8845, K.T. 07.04.2014.

Yargıtay'ın 25.12.2019 tarihli bir diğer kararında ise;

> "Sanığın, eski eşi olan mağdura ait facebook şifresini bildiğini ve şifre kırma gibi bir eyleminin olmadığını beyan etmesi, mağdurun, şifresinin kırılarak facebook hesabına giriş yapıldığına dair iddialarını doğrulayan herhangi bir delil bulunmaması karşısında, sanığın sübut bulan bilişim sistemindeki mağdura özel kısma girip, hakkı olmadığı halde sistemde kalmaya devam etme eyleminin TCK'nin 243/1. madde ve fıkrasındaki bilişim sistemine girme ve mağdura ait içeriği özel mesajları okuyup, tarafı olmadığı haberleşme içeriklerini kaydetmesi eyleminin TCK'nin 132/1. madde ve fıkrasındaki haberleşmenin gizliliğini ihlal suçlarını oluşturacağı gözetilmeden, delillerin takdirinde ve suç vasfında yanılgıya düşülerek, sanık hakkında TCK'nin 244/2. madde ve fıkrasındaki sistemi engelleme, bozma, verileri yok etme veya değiştirme ve TCK'nin 136/1. madde ve fıkrasındaki verileri hukuka aykırı olarak verme veya ele geçirme suçlarından mahkûmiyet kararı verilmesi"

bozma nedeni yapılmıştır.[65]

Yukarıda zikredilen Yargıtay kararları ışığında bir analiz yapmak gerekirse fail, bilişim sistemine hukuka aykırı şekilde girmiş olsa da şifre kırma ya da değiştirme bir faaliyet gerçekleştirmediği takdirde isnat edilen fiil, TCK'nin243. maddesinde yer alan bilişim sistemine girme suçudur. Bu fiilin, TCK' da yer alan diğer suçları da oluşturması durumunda somut olayın özelliğine göre mahkeme tarafından inceleme yapılmalıdır. Yargıtay'ın konuya ilişkin 01.06.2020 tarihli bir kararında,

> "Sanıkların …… Esnaf ve sanatkarlar odası üyelerine ait ellerindeki bilgilerin doğruluğunu teyit etmek için Nüfus ve Vatandaşlık İşler Genel Müdürlüğü ile anlaşma yapıp ücreti karşılığı yararlanmak yerine bir yazılım ile müşteki şirketin bilişim sistemine veri gönderip, seri şekilde milyonlarca sorgu yapıp sistemde var olan verileri aldıkları anlaşıldığından sanıkların eyleminin 5237 sayılı TCK' nun 244/2-4 maddelerinde düzenlenen suçu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemine girme suçundan mahkumiyetlerine karar verilmesi"

bozma nedeni sayılmıştır. Yargıtay'ın konuya ilişkin diğer bir kararında;

[65] Yargıtay 12. CD, E. 2019/577, K. 2019/12248, K.T. 25.12.2019.

> "Sanık hakkında bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan verilen hüküm açısından; dosya kapsamına göre sanığın, katılan M.T'nin elektronik posta adresinin ve facebook hesabının şifrelerini kırarak, hesaba giriş şifresini değiştirerek erişimini engellemesi şeklinde gerçekleşen eyleminin TCK'nin 244/2. maddesi kapsamında kaldığı halde suç vasfında hataya düşülerek aynı yasanın 243/1. maddesinden mahkûmiyet hükmü kurulması" [66]

bozma nedeni yapılmıştır. Bu kararda, failin kastının, yerel mahkeme tarafından TCK m.243 ve 244. maddeleri yönünden ayrı ayrı değerlendirilmesi gerektiği belirtilmiştir.

B) FİİL

5237 sayılı TCK'nin 243. maddesinin ilk fıkrası uyarınca bilişim sisteminin tamamına ya da bir kısmına hukuka aykırı olarak girmek ya da bu sistemde kalmaya devam etmek fiillerinin gerçekleşmesi gerekmektedir. Anılan hükümde 6698 sayılı Kanun'un 30. maddesi ile yapılan değişiklikle bu fıkrada yer alan *'ve'* ibaresi *'veya'* şeklinde değiştirilmiştir.[67] Bunun sonucu olarak failin bilişim sistemine hukuka aykırı olarak girmesi ya da bilişim sisteminde kalmaya devam etmesi ile suç tamamlanmaktadır.[68] Bilişim sisteminde kalma ya da sistemde kalmaya devam etme hareketi açıkça "ihmali" bir harekettir. Bu seçimlik hareketlerden birinin ihmali davranışla gerçekleştirilmesi ile suç tamamlanmaktadır.[69] Bu değişiklik yapılmadan önce suçun oluşması için sisteme girme eyleminin ve sistemde kalmaya devam etme eyleminin birlikte gerçekleşmesi koşulu aranmaktaydı.[70]

Anılan hükümde adı geçen girme ya da orada kalma fiili, bilişim sistemindeki mekanizmaya dahil birtakım ayarların açılması sonucu fiziken sisteme entegre olunması şeklinde algılanmamalıdır. Burada kastedilen aktif konumdaki bilişim sistemi aracı ile fail tarafından sanal ortama girmek

[66] Yargıtay 15. CD, E. 2017/3013317, K. 2018/2657, K.T. 04. 2018.

[67] İhtiyaroğlu, "Bilişim," 422.

[68] Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 4. Baskı, (Ankara: Seçkin Yayıncılık, 2014), 55.

[69] Tezcan, Erdem ve Önok, *Teorik ve Pratik Ceza Özel Hukuku,* 1150.

[70] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, 106.

anlaşılmalıdır. Dolayısıyla fail, aktif haldeki bilişim sistemine dahil olduğu için üçüncü kişilere ait özel veriler hakkında bilgi sahibi olabilmektedir.[71] Böylece bilişim sisteminin yazılımla ilgili bölümünün tamamına ya da bir bölümüne ulaşılması ile isnat edilen fiil gerçekleşmektedir.[72]

Bu hüküm ile bilişim sisteminde yazılım güvenliğini sağlamak amacı ile sistem kullanıcılarının mağduriyetinin önüne geçilmek istenmiştir.[73] Sözgelimi bir kimsenin rızası ile girilen bilişim sistemindeki verilerin hukuka aykırı olarak kopyalanması halinde de bu suç oluşabilir. Bunun yanı sıra kablosuz bir ağ aracılığıyla bilişim sisteminde üçüncü şahsa ait verilerin görüntülenmesi ile de bu suçun işlendiği görülmektedir. Ayrıca banka yetkilisinin, müşterinin hesabına onun bilgisi ve rızası olmadan hukuka aykırı olarak bakması da bu suç kapsamında değerlendirilmelidir.[74]

TCK'nin 243. maddesi kapsamında yer alan bilişim sistemine girme ya da bilişim sisteminde kalma suçunun, sıklıkla bir bilişim sistemine sahibinin rızası olmaksızın izinsiz bir şekilde uzaktan ya da ağ üzerinden gizli bir erişimle işlendiği görülmektedir. Bu erişimin en sık kullanılan metotlarından birisi de *"casus yazılım"*dır. Ayrıca dünyaca ünlü internet sitelerinin dahi siber saldırıya, değişik metotlar uygulanarak maruz kaldığı gerçeğini de göz ardı etmemek gerekir.[75]

Bilişim sistemine hukuka aykırı olarak girme metotları arasında solucan ve truva atı gibi çeşitli bilgisayar virüsleri bulunmaktadır. Buna bağlı olarak hem özel hem de kamu kuruluşlarının birtakım güvenlik uygulamaları aşılmak sureti ile bilişim sistemlerine girme ya da orada kalma suçu işlenmektedir. Bu durum, kamu kuruluşlarının ya da üçüncü kişilerin şifreleri ve diğer özel verileri ele geçirildiği için web sayfası hırsızlığının oluşmasına neden

[71] Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi," 415.

[72] Erdoğan, "Bilişim," 1398.

[73] Serkan Gönen, Halil İbrahim Ulus ve Ercan Nurcan Yılmaz, "*Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme*," *Bilişim Teknolojileri Dergisi 9,* no. 3, (2016): 232.

[74] B. Zakir Avşar ve Gürsel Öngören, *Bilişim Hukuku*, (İstanbul: Türkiye Bankalar Birliği, 2010), 17.

[75] Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*, 207.

olmaktadır. Bunun dışında bilişim sisteminde kullanımı münhasıran özel üyeliğe bağlı olan bir internet sitesine üye olunmadığı halde hukuka aykırı olarak girmek de TCK'nin 243. maddesi uyarınca bu suç türü kapsamına girmektedir.[76]

5237 sayılı TCK'nin 243. maddesinde öngörülen suçu oluşturan seçimlik hareketler yönünden isnat edilen suçun oluşumu için bir neticenin gerçekleşmesine gerek duyulmadığı görülmektedir. Bunun nedeni ise suçun oluşumu için anılan maddede yer alan bilişim sisteminin tamamına ya da bir kısmına girme ya da orada kalma şeklindeki seçimlik hareketlerin yapılmasının gerekli ve yeterli olduğu anlaşılmaktadır. Buna karşılık doktrinde suçun serbest hareketle işlenebilen bir suç olduğu da ifade edilmektedir. Bu suçların oluşması için herhangi bir verinin elde edilmesi de gerekmemektedir.[77] Dolayısıyla bu hükümdeki suç, sırf hareket suçu şeklinde tanımlanmaktadır. Bu nedenle failin fiili sonucunda bir zararın gerçekleşmesi aranmamaktadır. Ayrıca sistemin tehlikeye uğramasına yönelik bir saldırı tehdidinin bulunmasına da gerek yoktur. Bu özellikleri nedeni ile bilişim sistemine hukuka aykırı olarak girme ya da orada kalma, soyut bir tehlike suçunu oluşturmaktadır.[78]

Bilişim sistemine bir kimse, kasıtlı olmaksızın izinsiz olarak erişmekle birlikte hata yaptığını anlayıp hemen sistemden çıkar ise TCK'nin 243. maddesinin öngördüğü bu suç, failin kastının bulunmaması nedeniyle cezai sorumluluktan söz edilemez. Buna karşılık Yargıtay'ın bir kararında "*Sanığın, sübut bulan bilişim sistemine girip, katılan adına başkaları ile konuşma yapacak kadar kalmasından ibaret eyleminin TCK'nin 243/1. maddesinde tanımlanan "Bilişim Sistemine Girme" suçunu oluşturacağı gözetilmeden, TCK'nin 244/2. maddesinden hüküm kurulması kanuna aykırılık oluşturmaktadır.*[79]

Bilişim sistemi sahibinin rızası olmaksızın başkasının rızası hilafına konuşma yapmanın anılan hükme göre suç oluşturacağı vurgulanmıştır.

[76] İhtiyaroğlu, "Bilişim," 412.

[77] Tezcan, Erdem ve Önok, *Teorik ve Pratik Ceza Özel Hukuku*, 1153.

[78] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 341.

[79] Yargıtay, 12. CD, E. 2013/11510, K. 2014/2982, K.T. 10. 02. 2014.

C) NETİCE VE NEDENSELLİK BAĞI

5237 sayılı TCK'nin 243. maddesinde düzenlenen bilişim sistemine girme ya da orada kalma suçunun işlenebilmesi için hukuka aykırı olarak bir bilişim sisteminin bütününe ya da bir bölümüne girilmesi ya da orada kalınması gerekmektedir. Bu suç, daha önce birden fazla hareketin birbirine bağlı olarak yapılmasının zorunlu bulunduğu çok hareketli suç ya da birden fazla suç iken 6698 sayılı kanunun 30. maddesinde yapılan değişiklikle; seçimlik hareketli suça dönüştürülmüştür. Daha önce de belirtildiği gibi doktrinde suçun serbest hareketle işlenebilen bir suç olduğu da ifade edilmektedir. Bu suçların oluşması için herhangi bir verinin ele geçirilmesi koşulu da aranmamaktadır.[80] Bu düzenleme sonrasında bir kimse, bu yönde bir kastı bulunmayıp üçüncü kişinin bilişim sistemine girmesinin ardından yaptığı hataya rağmen hukuka aykırı bir şekilde sistemde kalmaya devam ediyor ise suç olarak kabul edilecektir.[81]

Bilişim sistemine hukuka aykırı olarak girme ya da bilişim sisteminde kalma fiili ile anlaşılması gereken bu sistemin sanal ortamına dahil olunarak bilişim sisteminin yazılımına erişilmesidir. Bu suç, üçüncü kişinin bilgisayar, tablet ya da mobil cihazlarındaki verilerinin, izinsiz olarak görüntülenmesi şeklinde oluşabileceği gibi herhangi bir ağda bilişim sistemine ait oturumun açılması yolu ile de işlenebilir.[82] Dolayısıyla suçun oluşumu, bilişim sisteminde kişisel verilerin ele geçirilmesi şartına bağlı değildir. Ayrıca bilişim sisteminde hukuka aykırı olarak kalınmaya devam edilmesi konusunda asgari bir süre şartı bulunmamaktadır. Bu konuda doktrinde baskın görüş, failin bilişim sistemine girdiğini anladığı halde sistemden çıkmaması, suçun oluşumu açısından yeterli görülmektedir. Bunun yanı sıra bilişim sistemine girilip girilmediği ya da hukuka aykırı şekilde sistemde kalınmaya devam edilip edilmediği somut olayın özelliğine göre analiz edilmelidir. Sonuç olarak bilişim sistemine hukuka aykırı olarak girilmesi ya da orada kalmaya devam edilmesi nedeni ile mağdur yönünden herhangi bir zararın meydana gelmemesi, suçun ortaya çıkmasına engel teşkil etmemektedir.[83]

[80] Tezcan, Erdem ve Önok, *Teorik ve Pratik Ceza Özel Hukuku*, 1153.

[81] Koca ve Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* 812.

[82] İhtiyaroğlu, "Bilişim," 425.

[83] Erdoğan**,** "Bilişim," 1377.

D) NİTELİKLİ HALLER

Suçun nitelikli hali denildiğinde cezanın daha az ya da daha fazla verilmesini gerektiren hal akla gelmelidir. Aşağıda belirtildiği gibi suçun varlığını etkilemeyen nitelikli haller, suçun basit şekline yapılan eklemelerdir.[84] Bu eklerle suçun basit şekli genişletilmekte ve faile verilecek ceza oranı azalmakta ya da artmaktadır.[85] Çalışmamızda öncelikli olarak daha az cezayı gerektiren haller konusunu ele alacağız.

1- Daha Az Cezayı Gerektiren Haller

5237 sayılı TCK'nin 243. maddesinin ikinci fıkrası uyarınca hukuka aykırı olarak bilişim sistemine girme ya da sistemde kalmaya devam etme suçuna cezanın daha az verilmesini gerektiren nitelikli hal düzenlenmiştir. Anılan hükme göre "hukuka aykırı olarak bilişim sistemine girme ya da sistemde kalma" fiillerinin, "*bedeli karşılığı yararlanılabilen sistemler*" hakkında işlenmesi, cezanın daha az verilmesini gerektiren nitelikli hal şeklinde düzenlenmiş ve işlenen fiile verilecek cezanın yarı oranında indirileceği öngörülmüştür.[86]

Bu düzenleme ile ücret karşılığı hizmet veren bilişim sistemlerine hukuka aykırı şekilde bedelsiz olarak girme halinde failin cezasında yarı oranda indirime gidilebileceği belirtilmiştir.[87] Sözgelimi internet ortamında ücret karşılığında şifreli erişimin sağlandığı, dergi, eğlence, sosyal medya ve yazılım gibi sistemlere şifrenin kırılarak girilmesi ya dabu sistemde kalınması, suçun daha az cezayı gerektiren sorumluluk halinin tipik bir örneğidir.[88]

Bu hüküm ile bilişim sistemine hukuka aykırı olarak girme ya da orada kalmaya devam etme fiilinin "*bedeli karşılığın yararlanılabilen sistemler*"

---

[84] Cengiz Apaydın, "Bilişim Sistemine Girme Suçu," *Türkiye Adalet Akademisi Dergisi* 7, no. 24 (Ocak 2016): 268.

[85] Hakan Hakeri, "Verileri Hukuka Aykırı Olarak Verme Suçu," (Tıbbi Müdahaleden Kaynaklanan Hukuki Sorumluluk Sempozyumu, 16-17 Ocak 2009, Mersin Barosu Yayını, Mersin 2009), 126.

[86] Tezcan, Erdem ve Önok, *Teorik ve Pratik Ceza Özel Hukuku*, 1154.

[87] Karakehya, "Türk," 17.

[88] Apaydın, "Bilişim," 269.

hakkında işlenmesi durumunda faile daha az ceza verilmesinin amacı, özel kişilere ait bir bilişim sistemine girmek ve orada kalmak halinde ihlal edilen hukuki yararın, bedeli karşılığında yararlanılan sistemlere girmek ya da orada kalma sonucu ihlal edilen hukuki yarardan daha fazla korunmaya değer olduğu argümanına dayanmaktadır.[89]

Doktrinde anılan hükümde zikredilen bir bedel karşılığı koşuluna bakılmaksızın kamu kurumlarının ya da kuruluşlarının, bilişim sistemlerine hukuka aykırı olarak girmenin ya da orada kalma suçunun, daha fazla cezayı gerektiren hal şeklinde düzenlenmesi gerektiği belirtilmektedir. Hatta kamu kurum ve kuruluşlarında isnat edilen bu fiil karşılığında verilecek cezanın, gerçek kişiler ile özel hukuk kişilerine karşı işlenmesi durumunda verilecek cezadan daha ağır olması gerektiği savunulmaktadır.[90]

5237 sayılı TCK'nin 163. maddesi uyarınca karşılıksız yararlanma suçu kapsamında bulunan otomatlar aracılığıyla sunulan ve ücret karşılığı yararlanılan sistemlere hukuka aykırı olarak girmek, bilişim sistemine girme ya da bilişim sisteminde kalma suçunu oluşturmamaktadır. Bunun dışında telefon hatları ya da elektromanyetik dalgalarla yapılan şifreli yayınları hukuka aykırı olarak izlemek, bu fiil kapsamına girmemektedir.[91]

2- Netice Sebebiyle Ağırlaşmış Hal

Bu konu, 5237 sayılı TCK'nin 243. maddesinin üçüncü fıkrasında düzenlenmiştir.[92] Anılan hüküm gereği; suçun işlenmesi sonucunda sistemin içerdiği veriler değişir ya da yok olur ise bu suç yönünden cezanın ağırlaştırılması zorunludur. Bu hüküm uyarınca, *"bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunacağı* belirtilmiştir.[93] Böylece verilerin yok olması veya değiştirilmesi ile bilişim sistemine girme suçunun, neticesi sebebiyle ağırlaşmış hali

[89] Kurt, *Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları,* 147.

[90] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, 110; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* 361.

[91] Eker, "Türk," 123.

[92] Malkoç, *Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu*, 1671.

[93] Eker, "Türk," 124.

gerçekleşmektedir.[94] Bunun sonucu olarak bilişim sistemine hukuka aykırı olarak girilmesi ya da orada kalmaya devam edilmesi sonucunda "*sistemin içerdiği veriler yok olur ya da değişirse"* ceza arttırılacaktır.[95]

Daha önce de değindiğimiz gibi bu durumda neticesi sebebiyle ağırlaşmış bir suç ortaya çıkmaktadır.[96] Dolayısıyla suç oluşturan bir fiili işlenildiği takdirde failin kastettiği neticeden daha ağır ya da farklı bir sonuç gerçekleşmiş olabilir. Burada fail, her ne kadar böyle bir neticenin gerçekleşmesini istemese de kastettiği netice dışında gerçekleşen daha ağır netice ya da farklı bir sonuç nedeni ile neticesi sebebiyle ağırlaşmış suç söz konusudur.[97]

Netice sebebiyle ağırlaşmış suç konusunu düzenleyen TCK'nin 23. maddesi uyarınca, "*Bir fiilin, kastedilenden daha ağır veya başka bir neticenin oluşumuna sebebiyet vermesi hâlinde, kişinin bundan dolayı sorumlu tutulabilmesi için bu netice bakımından en azından taksirle hareket etmesi gerekir*" ifadesine yer verilmiştir. Anılan hüküm uyarınca failin kastı, bilişim sistemine hukuka aykırı girme ya da orada kalmaya yönelik olmalıdır. Aksi takdirde sistemdeki verileri yok etme ya da değiştirmeye yönelik bir kastı bulunduğu takdirde bu hükmün uygulanması mümkün değildir. Buna karşılık failin bu yönde bir kastı olmasa dahi bilişim sistemine hukuka aykırı girmesi sonucu veriler yok olur ya da değişirse; failin ağırlatıcı nedenden sorumlu tutulabilmesi için en azından taksirli bir hareketinin bulunması gerekir.[98] Buna karşılık fail, bilişim sistemindeki verilerin engellenmesi, bozulması, yok olması ya da değişmesi kastıyla hareket ediyorsa TCK'nin 244. maddesi uyarınca, *"sistemi engelleme, bozma, verileri yok etme veya değiştirme*" fiilinden ötürü sorumlu olacaktır. Öte yandan fail, başkasının bilişim sistemine hukuka aykırı olarak girme ya da orada kalma fiilini işleyip

[94] Özbek, Doğan, Bacaksız ve Tepe, *Türk Ceza Hukuku Özel Hükümler*, 951.

[95] Özbek, Doğan, Bacaksız ve Tepe, Türk *Ceza Hukuku Özel Hükümler,* 951.

[96] Tezcan, Erdem ve Önok, *Teorik ve Pratik Ceza Özel Hukuku*, 1155.

[97] Sulhi Dönmezer ve Sahir Erman, *Nazari ve Tatbiki Ceza Hukuku II*, (İstanbul: Beta Yayınevi, 1997), 333.

[98] Yazıcıoğlu, "Yeni," 403.

bilişim sistemindeki verilere de zarar vermişse, netice sebebiyle ağırlaşmış hal gereği cezalandırılacaktır.[99]

Yargıtay 12. Ceza Dairesi 04.11.2013 tarihli bir kararı şu şekildedir:

> "TCK'nin 243/1 maddesinde, 'Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir'; aynı kanunun 243/3.maddesinde, 'Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur' şeklinde birbirinden farklı yaptırım içeren ve biri diğerinin neticesi sebebiyle ağırlaşmış halini oluşturan iki ayrı düzenlemeye yer verildiği gözetilmeden, bilişim sistemine hukuka aykırı olarak giriş yaptığı kabul edilen sanığın eylemi nedeniyle sistemden yok olan veya değişen veri ya da veriler hakkında bir açıklamada bulunulmaksızın ve TCK'nin 244/2. maddesinin uygulanabilirliği bakımından kabul edilen bu neticenin sanık tarafından kasten meydana getirilip getirilmediği de irdelenmeksizin, 'Sanığın bilişim sistemine girme suçundan eylemine uyan TCK 243/1-3 maddesi gereğince suçu işleyiş şekli dikkate alınarak takdiren: ALTI AY HAPİS CEZASI İLE CEZALANDIRILMASINA şeklinde, TCK'nin 243. maddesinin her iki fıkrası da hükümde gösterilip, yasal yeterli ve geçerli bir gerekçeye dayanılmadan, sanığın bilişim sistemine girme suçundan mahkumiyetine karar verilmesi…"[100]

VI. HUKUKA AYKIRILIK

5237 sayılı TCK'nin 243. maddesinin birinci fıkrası gereği; *"bir bilişim sisteminin bütününe ya da bir bölümüne hukuka aykırı olarak giren ya da bu sistemde kalmaya devam eden"* bu suç nedeniyle cezalandırılmaktadır. Bu hükümden de anlaşıldığı gibi anılan suçun kanuni tanımında hukuka aykırılığın bulunması gerektiği zikredilmiştir. Bunun dışında bilişim sistemi üzerinde hak sahibi, kimi durumlarda failin bu sistemin bir bölümüne girmesine rıza göstermiş ise bu durumda failin hak sahibinin rızası dışındaki alanlara girmesi hukuka aykırılık oluşturacak ve bu suç işlenmiş olacaktır. Bu konuda verilen rıza bilişim sistemi üzerinde hak sahibi olan kişi tarafından

[99] Eker, "Türk," 124.

[100] Yargıtay 12. CD, E. 2012/31498, K. 2013/24496 aktaran Muhammed Sefa Çetin; "Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu (TCK m.243)", *Türkiye Adalet Akademisi Dergisi* 12, no. 45, (Ocak 2021): 18.

verilmez ise yetkili olmayan birisi tarafından verildiği için hukuken geçerli olmayacaktır.[101]

Hukuka aykırılık konusunda fail, bir bilişim sistemine girmesi ya da bu sistemde kalması hususlarında hataya düşer ise bu hatasından yararlanması mümkün olabilir. Bu konuda TCK'nin 30. maddesinin birinci fıkrası uyarınca hukuka uygunluk nedenleri çerçevesinde maddi koşullar bakımından kaçınılmaz bir hataya düşen failin hukuken sorumluluğun olmadığı kabul edilmelidir. Bunun dışında failin işlediği fiilin suç oluşturduğu hususunda hataya düşmesi de ihtimal dahilinde olabileceği için bu hususta da TCK'nin 30. maddesinin üçüncü fıkrası uyarınca hukuka uygunluk nedenlerinin varlığı yönünden kaçınılmaz bir hataya düşüp düşmediğinin mutlaka incelenmesi gereklidir.[102]

TCK'nin öngördüğü şekilde kanunların verdiği yetkiye dayanılarak izinsiz olarak bilişim sistemine girilmesi ya da bilişim sisteminde kalınması da hukuka uygunluk nedenidir. Bunun dışında 5271 sayılı CMK'nin 134. maddesinde belirtilen "*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma",* anılan kanunun 135. maddesinde yer alan *"İletişimin Tespiti, Dinlenmesi ve Kayda Alınması"* ve bu kanunun 140'ıncı maddesinde öngörülen *"Teknik Araçlarla İzleme"* koruma tedbirleri, kanunda belirtilen şartlara uygun olarak icra edilir ise suç olarak kabul edilmeyecektir. Buna karşılık yetkili kişilerce girilmesi zorunlu bir internet programı ya da web sayfasına fail tarafından hukuka aykırı şekilde şifrenin kırılması sonucu erişilmiş ise bu suç işlenmiş sayılacaktır. Böylece fail tarafından şifre aranan bir sisteme, yetkisiz olarak şifrenin kırılması sonucu erişim sağlandığı için bilişim sistemine hukuka aykırı şekilde girilmektedir.[103]

Bir bilişim sisteminin açık konumda olması ya da şifre konulmaması, bilişim sistemi üzerinde hak sahibinin rıza gösterdiği şeklinde değerlendirilmemelidir. Bu konuda evine teslim etmesi için emanet olarak arkadaşından aldığı bilgisayarın şifresiz açılarak sisteme girilmesi durumunda hak sahibinin

[101] İhtiyaroğlu, "Bilişim," 427.

[102] Büşra Özçelik, "Bilişim Sistemine Girme Suçu," (Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2019), 73.

[103] Karakehya, "Türk," 17.

rızası bulunmamaktadır. Dolayısıyla hak sahibinin rızasının, fiil öncesinde bulunması zorunludur. Bunun dışında rızanın şarta bağlı olarak verilip verilmeyeceği konusunda doktrinde farklı görüşler yer almaktadır. Bu konuda bazı yazarlar, bilişim sistemine başlangıçta belirli bir amaç doğrultusunda sisteme girilmesi için verilen rıza nedeni ile bu sistemin farklı bir amaçla kullanılmasının suç kapsamına girmeyeceğini öne sürmektedir.[104] Doktrinde baskın görüş ise bilişim sisteminin sahibinin öngördüğü amaç dışında sistemin kullanılmasının suç olduğunu savunmaktadır. Buna gerekçe olarak da hak sahibinin, burada gerçekleşen fiiller yönünden rızasının bulunmadığı zikredilmektedir. Sözgelimi hak sahibinin, faile cep telefonunu, sadece bir yakınına mesaj gönderebilmesi amacıyla verdiği halde failin, hak sahibine ait cep telefonundaki özel fotoğrafları görmesi ya da telefondaki özel programları incelemesi tarzındaki fiiller, bilişim sistemine girme ya da orada kalınması suçunun tipik örneğidir.[105]

VII. MANEVİ UNSUR

TCK'nin 243. maddesinin birinci fıkrası gereği*; "bilişim sisteminin tamamına ya da bir bölümüne girme ya da sistemde kalma suçu",* yalnızca kasten işlenebilmektedir. Bunun sonucu olarak failin kasıtlı olarak bir bilişim sisteminin tamamına ya da bir bölümüne girmesi ya da bu sistemde bilerek ve isteyerek kalması halinde suç gerçekleşmektedir.[106] Bu konuyla ilgili olarak Avrupa Konseyi Siber Suçlar Sözleşmesi'nin ikinci maddesi gereği, sözleşmeye taraf ülkelerin "*bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman*" bu fiilden ötürü cezai yaptırımı uygulamaları öngörülmüştür. Bu düzenleme ile TCK'nin 243. maddesinin birinci fıkrası arasında paralellik olduğu görülmektedir.[107]

Anılan hüküm uyarınca isnat edilen fiilin hangi amaçla işlendiğinin herhangi bir önemi yoktur. Bunun sonucu olarak fail tarafından kasıtlı şekilde hareket edilmesi suçun oluşumu yönünden gerekli ve yeterlidir. Dolayısıyla

[104] Gönen, Ulus ve Yılmaz, "Bilişim,". 235.

[105] İhtiyaroğlu, "Bilişim," 428.

[106] Koca ve Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* 814.

[107] Erdoğan, "Bilişim," 1405.

failin kasıtlı hareket etmesi koşulu ile deneme ya da başka bir saikle bu suçu işlemesinin herhangi bir önemi bulunmamaktadır. Buna karşılık TCK'nin 243. maddenin üçüncü fıkrasında yer alan suçun neticesi sebebiyle ağırlaştırılmış halinde, verilerin yok olması ya da değiştirilmesi durumunda fiilin en azından taksirle gerçekleşmesi gereklidir. Şayet burada fail, kasıtlı bir şekilde verileri değiştirmiş ya da bozmuş ise TCK'nin 244. maddesi uyarınca sorumluluğu olacaktır.[108]

Anılan maddenin dördüncü fıkrası yönünden de tıpkı birinci fıkradaki kast aranmaktadır. Bu konuda Türk Ceza Kanunu'nda failin taksirli fiilinin cezalandırılacağına yönelik bir hüküm olmadıkça o suçtan doğan cezai sorumluluğu bulunmamaktadır. Ayrıca TCK'nin 243. maddesinin üçüncü fıkrası dışında suçun gerçekleşmesi için failde doğrudan kast iradesi aranmaktadır.[109] Bunun dışında fail, bilişim sistemine yönelik icra hareketlerine başlamış olmakla birlikte icra hareketlerini tamamlamadan önce sisteme girmekten vazgeçer ise gönüllü vazgeçmeden yararlanabileceği öngörülmektedir.[110]

VIII. SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ

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

A) TEŞEBBÜS

Bilişim sistemine girme ya da bilişim sisteminde kalma suçunun niteliği, seçimlik hareketli bir suç olması nedeni ile teşebbüs açısından doktrinde fikir birliğine ulaşılabilmiş değildir. Bazı yazarlar, bu suçun, soyut tehlike suçu niteliğinde olması nedeni ile teşebbüse elverişli olmadığını öne sürmektedir. Buna gerekçe olarak da failin bilişim sisteminin tamamına ya da bir bölümüne hukuka aykırı olarak girmesi ya da bu sistemde kalma fiilini

[108] Karakehya, "Türk," 14.

[109] Gönen, Ulus ve Yılmaz, "Bilişim," 230.

[110] Karakehya, "Türk," 14.

işlediği anda suçun tamamlandığı argümanına dayanmaktadır.[111] Buna karşılık bazı yazarlar ise bilişim sistemine girme suçunda girme ya da kalma fiillerinin, farklı bir şekilde değerlendirilmesi gerektiğini vurgulamaktadır.[112]

Bilişim sistemine kalma fiili yönünden fail, bilişim sistemine hukuka aykırı olarak girmiş ise kalma fiili açısından teşebbüsün varlığından söz edilemez. Dolayısıyla fail, hukuka aykırı olarak erişim sonucunda bilişim sistemine girmesinin ardından çok az bir süre kalsa bile suç işlenmiş sayılacaktır.[113] Bunun dışında TCK'nin 243. maddesinin üçüncü fıkrası uyarınca, fail, bilişim sistemine hukuka aykırı olarak girmesi sonucu verileri yok eder ve değiştirir ise artık burada taksirli bir fiil ile suç gerçekleştiği için teşebbüsten söz edilemeyecektir.[114] Buna karşılık doktrinde baskın görüş, bilişim sistemine girme fiilinin, teşebbüse elverişli nitelikte bir suç olmasıdır.[115] Kanaatimizce de fail, bilişim sistemine girme fiili yönünden iradesi dışında gelişen kimi nedenler ile sisteme erişim sağlayamamış ise bu durumda teşebbüsün varlığından söz edilebilir. Sözgelimi failin, mağdura e-posta ile *trojan* olarak da adlandırılan kötü amaçlı program göndermesi durumunda bilişim sistemi sahibi, virüs içeren programı açmaz ya da siler ise bu sisteme girilememesi yüzünden suç, teşebbüs aşamasında kalacaktır.

Yargıtay'ın 21.01.2014 tarihli bir kararında;

> "Şüphelilerin kurdukları "www.unimugla.com" adlı internet sitesinin giriş sayfasını, müşteki Muğla Üniversitesi'nin "Dijital Üniversite" adlı internet sitesinin giriş sayfası ile aynı yaparak, kendi sitelerini Dijital Üniversite sitesi sanarak bu siteye parola v.s. bilgilerini giren kullanıcıların bu bilgilerini elde ederek, Muğla Üniversitesinin yasal internet sitesi olan Dijital Üniversite sitesine haksız yere girerek buradaki bilgileri elde etmeye ve yine kullanıcıların gerçek bilgilerini kullanarak dolandırıcılık suçunu işlemeye çalıştıkları iddia olunan

[111] Sacit Yılmaz, *Türk Ceza Hukuku Sisteminde Siber Suçlar*, (Ankara: Adalet Yayınevi, 2016), 190.

[112] Koray Doğan, "Bilişim Suçları ve Yeni Türk Ceza Kanunu," *Hukuk ve Adalet Eleştirel Hukuk Dergisi*, no. 6-7, (2005): 298.

[113] Akbulut, "Bilişim," 150-151.

[114] Özbek, Doğan, Bacaksız ve Tepe, *Türk Ceza Hukuku Özel Hükümler,* 955.

[115] Erdoğan, "Bilişim," 1413-1414.

> olayda, sanıkların bu site ile herhangi bir şifreyi kopyalama veya öğrenme imkânlarının bulunmadığı, iddia edilen amaca ulaşmaya yarar uygun vasıtalar içermediği, gerek dolandırıcılık gerekse bilişim sistemine girme ya da bu suçlara teşebbüs etme suçlarını işlemeye elverişli araçlar bulunmadığı, sanıkların üzerine atılı bulunan iddiaların eylemlerinin gelecekte tehlike yaratabileceği kaygısına dayandığı, mahkûmiyete yeterli delil bulunmadığı gerekçeleriyle mahkemece verilen beraat kararında bir isabetsizlik görülmemiştir."[116]

ifadesine yer verilerek failin kastı, bilişim sistemine hukuka aykırı olarak girme ya da orada kalmaya devam etme suçu yönünden elverişli hareketlerle fiilin icrasına doğrudan başlanmaması nedeni ile teşebbüsten söz edilemeyeceği belirtilmiştir.

5237 sayılı Türk Ceza Kanunu'nun243. maddesinin dördüncü fıkrasında öngörülen "*bilişim sistemindeki veri nakillerinin sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlenmesi*" suçunun, teşebbüse elverişli olduğu ifade edilebilir. Anılan hükümde zikredilen veri nakillerinin teknik araçlarla izlenmesi, devamlılık arz ettiği için mütemadi suç niteliğindedir. Buna bağlı olarak fiil devam ettiği sürece suçun kesintiye uğramasından söz edilemez. Burada suçta teşebbüsten söz edebilmek için fail tarafından fiile elverişli hareketlerle doğrudan başlanılması ve suçun henüz tamamlanmaması gereklidir. Bu nedenle veri izleme faaliyeti aşamasında fail, iradesi dışında engellenmiş ya da veri nakillerini ve transferlerini takip etme olanağı bulamamış ise bu durumda teşebbüs söz konusudur.[117]

Fail, bilişim sistemine hukuka aykırı olarak girmek istese bu sisteme girmekten son anda özgür iradesi ile vazgeçer ise TCK'daki gönüllü vazgeçme hükmünden yararlanabilir. Bu durumda failin, daha önce de değindiğimiz gibi Türk Ceza Kanunu'nun 243. maddenin birinci fıkrası uyarınca sorumluluğu bulunmamaktadır.[118]

[116] Yargıtay, 11. CD, E. 2012/13233, K. 2014/795, K.T. 21. 01. 2014.

[117] Koca ve Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* 823.

[118] İhtiyaroğlu, "Bilişim," 430.

B) İŞTİRAK

TCK m.243'te düzenlenen bilişim sistemine girme ya da orada kalma suçu, birden fazla kişi tarafından iştirak halinde işlenebilir. Bu nedenle, bilişim sisteminin bir kısmına veya bütününe hukuka aykırı olarak girme ya da orada kalma suçu iştirak halinde işlendiği takdirde bu konuya ilişkin olarak 5237 sayılı TCK'nin (m.37-41) hükümleri uygulanacaktır.[119]

Bu suçun, başka birini bilişim sistemine girmeye ya da orada kalmaya ikna etme şeklinde gerçekleşmesi durumunda kişi, azmettiren sıfatı ile sorumlu olacaktır. Dolayısıyla bilişim sistemleri hakkında yeterli bilgisi olmadığı için bu hususta yetkili bir arkadaşını, sisteme girme konusunda ikna eden ve bu fiilin gerçekleşmesini sağlayan kimse TCK'nin 38. maddesi uyarınca azmettiren sıfatı ile sorumlu olacaktır. Öte yandan bilişim sistemine giren kimse ise TCK'nin 37. maddesi çerçevesinde suçun faili olarak sorumlu tutulacaktır.[120]

Suçun işlenmesinde faile "*yardım eden*" sıfatıyla da katılmak söz konusu olabilir. Sözgelimi bilişim sistemine erişim olanağı bulunmayan kimselere, şifre kırma programı sağlamak sureti ile failin, bilişim sistemine hukuka aykırı olarak erişim sağlaması durumunda TCK'nin 39. maddesi uyarınca iştirak iradesinin de bulunması şartı ile bu kişi, yardım eden sıfatıyla sorumlu tutulacaktır. Yine bilişim sistemine hukuka aykırı olarak giren ya da orada kalmaya devam eden faile, erişimi sağlayan servis sağlayıcıları da iştirak iradesinin bulunması şartı ile suça iştirakten sorumlu kılınabilir.[121] Yasa dışı erişimin sağlanmasında erişim sağlayıcılar da suç işleme kastı ve iştirak iradelerinin bulunması şartıyla, suça iştirakten sorumlu tutulabilecektir.[122]

İstanbul Bölge Adliye Mahkemesi tarafından verilen bir kararda "Şüphelinin diğer şüpheli tarafından azmettirmesi ve talimatı sonucu, "*… Medikal Ürün. San. ve Tic. Ltd. Şti. ünvanlı firmada çalıştığı sırada müştekinin kullanımına tahsis edilen bilgisayardan, hukuka aykırı olarak ve bu bilinçle, müştekinin şahsi e-posta hesabına müştekinin izni ve haberi olmaksızın*

[119] Çetin, "Yargıtay," 19.

[120] Apaydın, *Bilişim Suçları ve Bilişim Ceza Hukuku*, 288.

[121] Çetin, "Yargıtay," 20.

[122] Erdoğan, "Bilişim," 168.

erişerek ve burada kalarak bu hesaptaki şirkete ilişkin yazışmaların içeriğini ele geçirdiği ve böylece üzerlerine atılı bulunan suçu iştirak halinde işledikleri ve atılı suçun unsurları itibari ile oluştuğuna kanaat getirilerek" bilişim sistemine girme suçundan mahkumiyet kararı verilmiştir.[123] Bu kararda, failin, müştekinin rızası dışında bilişim sistemine girmek suretiyle e-posta hesabındaki verilere erişmesi, bilişim sistemine girme suçunu oluşturmuştur. Bu suçun, iştirak halinde işlendiği sonucuna varılmış ve faili suç işleme konusunda yönlendiren kişinin de *"azmettiren"* olarak sorumlu olacağı hükme bağlanmıştır.[124]

C) İÇTİMA

Suçların içtimaı konusu bilindiği gibi TCK'nin 42, 43 ve 44. maddelerinde düzenlenmiştir. Anılan kanunun 43. maddesinde zincirleme suç düzenlenmiştir. Bu hükme göre fail, suç işleme kastıyla değişik zaman dilimlerinde bir kişiye karşı aynı suçun temel şeklini ya da nitelikli hallerini işler ise zincirleme suçtan söz edilebilir. Bilişim sistemine girme ya da sistemde kalma suçu yönünden TCK'nin 243. maddesinin birinci ve üçüncü fıkraları uyarınca zincirleme suç hükümleri uygulanır. Bu bağlamda failin, başkasına ait bilişim sisteminin tamamına ya da bir bölümüne hukuka aykırı olarak farklı zamanlarda girmesi durumunda zincirleme suç oluşur ve failin cezası dörtte birden dörtte bir ila dörtte üç oranına kadar arttırılabilir.[125]

Bu suçun işleniş tarzı özellikle zincirleme suç hükümlerinin uygulanması, failin hukuka aykırı olarak bilişim sisteminde kaldığı süreye bağlıdır. Bu süre, failin aynı suç işleme kastıyla hareket edip etmediğini belirleyen en önemli ölçüttür. Doktrinde bu konuda bazı yazarlar, gerçek içtima hükümleri uygulanması için failin aynı suç işleme kastıyla hareket etmesine olanak tanımayacak derecede yani bilişim sisteminde uzun süre kalmasının gerekli olduğunu savunmaktadır.[126] Bunun sonucu olarak fail yönünden, sistem sahibinin rızası dışında hukuka aykırı biçimde sisteme her erişimi

[123] İstanbul BAM 26. CD, E. 2019/141, K. 2019/368 kararı, aktaran İhtiyaroğlu, "Bilişim," 431.

[124] İhtiyaroğlu, "Bilişim," 431.

[125] Akbulut, "Bilişim Suçları," 152.

[126] Erdoğan, "Bilişim," 1417.

için kendisi hakkında farklı bir cezai yaptırım uygulanacaktır. Buna karşılık bazı yazarlar ise fail çok kısa bir zaman diliminde bilişim sistemine hukuka aykırı olarak girmesi halinde dahi zincirleme suç hükümlerinin uygulanacağını ve bu suç nedeni ile sadece tek bir suç karşılığı cezanın arttırılması gerektiğini öngörmektedir.[127]

Bilişim sisteminde kalma fiili, süreklilik arz ettiği için mütemadi suçtur. Bu nedenle bilişim sisteminde kalma süresi kesintiye uğramadıkça fiilin tipikliği gereği failin kastının, tek suça yönelik olduğu şeklinde kabul edilmektedir. Buna karşılık faili, bilişim sistemine hukuka aykırı olarak girme ya da orada kalma fiilini değişik kişilere karşı işlemiş ise mağdur oranı kadar suç sayısı olacaktır.[128] Bu suç yönünden bileşik suç hükümleri uygulanabilir. Bu durumda bilişim sistemine girme ya da sistemde kalma suçu başka bir suçun unsuru ya da nitelikli halini oluşturabilir. Sözgelimi failin bilişim sistemlerini araç olarak kullanarak nitelikli dolandırıcılık suçunu işlemesi, bu duruma örnek olarak gösterilebilir.[129]

Bilişim sistemlerinin fail tarafından hukuka aykırı olarak kullanılması yoluyla mağdurun özel hayatının gizliliği ihlal edilir veya haberleşmesi engellenirse fikri içtima hükümleri uygulanacaktır. Aynı durum haberleşmenin gizliliğinin ihlali için de geçerlidir.[130] TCK 243 ve 244 arasındaki ilişkinin de açıklanması zorunluluğu bulunmaktadır. Doktrinde bir görüşe göre iki suç arasında fikri içtima hükümleri uygulanmalıdır.[131] Diğer bir görüşe göre ise failin kastına göre hareket edilmeli, 244. maddede yer alan suç olmuşmuşsa artık 243. maddeye göre ceza verilmemelidir.[132]

[127] Doğan Soyaslan, *Ceza Hukuku Özel Hükümler*, 11. Basım, (Ankara: Adalet Yayınevi, 2016), 638.

[128] Erdoğan, "Bilişim" 1417.

[129] İhtiyaroğlu, "Bilişim," 432.

[130] Meral Şahin Ekici ve Irmak Koruculu, "Bilişim Sistemine Girme Suçu, Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 21*, (Özel Sayı, 2019): 599.

[131] Koca ve Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* 819.

[132] İhtiyaroğlu, "Bilişim," 433.

TCK 243 ve 244 arasındaki bağı tüketen ve tükenen norm ilişkisi olarak kabul edenler olduğu gibi bu bağın bulunmadığını, eylemler arasındaki zamansal farka göre hareket edilmesi gerektiğini ileri sürenler bulunmaktadır.[133] Ankara Bölge Adliye Mahkemesi'nin bir kararında "*Dosyanın bir bütün halinde incelenmesinde, sanığın birden fazla kez aynı kast altında katılanın yetkilisi olduğu ve …Bilişim Sistemleri Ltd. Şti' nin internet sitesine girerek kendi savunmasına göre orada tespit ettiği güvenlik açıklarını firma yetkililerine göstermek amacıyla veri yerleştiği ve verileri bozduğu iddia edilmiş ise de, sanığın katılana ait bilişim sistemine izinsiz girdiği ancak veri yerleştirdiğine ve verileri bozduğuna dair delil bulunmadığından, sanığın eyleminin TCK'nın 244/2 maddesinde belirtilen bilişim sistemine izinsiz girerek veri yerleştirme ve bozma suçunu değil, sadece bilişim sistemine hukuka aykırı olarak girme suçunu oluşturduğu ve sanığın aynı suç işleme kararını icrası kapsamında değişik zamanlarda aynı mağdura karşı aynı suçu birden fazla kez işlediği, bu nedenle de hakkında zincirleme suç hükümlerinin uygulanması gerektiği*" belirtilmekle, suçun bilişim sistemine hukuka aykırı girilmesi olduğu, sisteme herhangi bir veri yerleştirilmediği ya da var olan verilerin bozulmadığı, bu nedenle TCK'nin 244. maddesinin 2. fıkrasında yazılı olan suçun somut olayda meydana gelmediği, failin bilişim sistemine girme suçundan zincirleme suç hükümlerine göre cezalandırılması gerektiği kabul edilmiştir.[134]

Yargıtay'ın konuya ilişkin bir kararında *"Sanık hakkında düzenlenen iddianamede; sanığın, mağdura ait facebook ve telefon hesaplarına rızası dışında girerek bilişim sistemine girme, mağdurun orijinal fotoğrafları ile birlikte çıplaklık içeren fotoğrafları mağdura aitmiş gibi internette paylaşarak görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçlarını işlediği iddia edilmiş olup, sanığa yüklenen farklı eylemlerden dolayı ayrı ayrı hüküm kurulması gerektiği, TCK'nin 44/1. madde ve fıkrasındaki fikri içtima koşullarının bulunmadığı gözetilmeden, "bilişim sistemlerine girme ve özel hayatın gizliliğini ihlal suçlarının sabit olmakla birlikte tek bir eylem ile icra edildiğinden TCK'nin 44. maddesinin bu suçlar yönünden tatbik edilmesine" biçimindeki yasal ve yeterli olmayan gerekçelerle yazılı şekilde görüntü veya seslerin ifşa edilmesi suretiyle özel*

[133] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 384.

[134] Ankara BAM 8. CD, E. 2017/207, K. 2018/439, K.T. 17.04.2018.

hayatın gizliliğini ihlal suçundan mahkûmiyet hükmü kurulması" bozma nedeni yapılmıştır.[135] Görüldüğü gibi failin fiili sonucu bilişim sistemine girme suçu dışında oluşan diğer suçlar bakımından inceleme yapılması gerektiği ifade edilmiş ve bu sonuca göre TCK'nin 44. maddesi çerçevesinde değerlendirilme yapılması gerektiği vurgulanmaktadır. Aksi takdirde fikri içtima hükümlerine uygun olmayan bir hüküm tesis edilecektir.[136]

IX. YAPTIRIM

5237 sayılı Türk Ceza Kanunu'nun 243. maddesinin birinci fıkrasında düzenlenen suçun temel şeklinin cezası, bir yıla kadar hapis ya da adli para cezası olarak belirlenmiştir. Bununla birlikte TCK'nin49. maddesinin birinci fıkrası hükmüne göre kısa süreli hürriyeti bağlayıcı cezanın alt sınırı bir aydır. Bu suça ilişkin olarak adli para cezasının da seçenek yaptırım olarak uygulanmasına karar verilebilir. Buna karşılık fail hakkında hürriyeti bağlayıcı cezanın verilmesine karar verildiği takdirde mahkeme tarafından TCK'nin58. maddesinin üçüncü fıkrası hükmü gereği bu ceza, adli para cezasına çevrilemeyecektir.[137]

Bu suç türü yönünden her ne kadar seçenek bir yaptırım olarak öngörülmüş olsa da TCK'nin 243. maddesinde adli para cezasına yönelik herhangi bir alt ve üst sınır oranı belirtilmemiştir. Bu konuyu düzenleyen TCK'ninm.61/9 f. hükmü uyarınca*; "adli para cezasına ilişkin gün biriminin alt sınırı, o suç tanımındaki hapis cezasının alt sınırından az; üst sınırı da hapis cezasının üst sınırından fazla olamayacaktır.*[138]

5237 sayılı TK'nin 243. maddesinin birinci fıkrası uyarınca, *bilişim sisteminin bir kısmına veya bütününe hukuka aykırı olarak girme veya orada kalma fiilleri sonucu sistemin muhteviyatını oluşturan veriler yok olursa veya değişirse, altı aydan iki yıla kadar hapis cezasına* hükmolunacaktır.

Anılan hükmün ikinci fıkrasında ise "*Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde,*

[135] Yargıtay 12. CD, E. 2018/8261, K. 2019/6852.

[136] İhtiyaroğlu, "Bilişim," 434.

[137] Tezcan, Erdem ve Önok, *Teorik ve Pratik Ceza Özel Hukuku,* 1146.

[138] Şahin Ekici ve Koruculu, "Bilişim," 622.

verilecek ceza yarı oranına kadar indirileceği" öngörülmektedir. *(TCK m.243/2)*

6698 sayılı kanunun 30. maddesinde 24.03.2016 tarihinde yapılan değişiklikle *Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı."* hükme bağlanmıştır (*TCK m.243/4).*

Anılan hükümde düzenlenen bilişim sistemine girme veya kalma suçu, takibi şikâyete bağlı bir suç değildir. Bu nedenle Cumhuriyet savcılığınca re'sen soruşturma ve kovuşturmanın yürütülmesi gereklidir.[139]

[139] Soyaslan, *Ceza Hukuku Özel Hükümler*, 642.

SONUÇ

Bilim ve teknolojinin baş döndürücü hızla gelişimine paralel olarak bilişim hukuku alanında ülkemizde ve dünyada hukuki düzenleme yapma zorunluluğu doğmuştur. Günümüzde; dijital iletişim araçlarının kullanımının yaygınlaşması ile bilişim sistemine girme ya da bilişim sisteminde kalma fiilleri, herkes tarafından kolayca işlenebilecek bir suç türü konumundadır. Bu suç, başta bilişim sisteminin güvenliği ve güvenilirliği olmak üzere kişisel veriler, kişilerin özel yaşamı, ticari alan, ulusal ve uluslararası güvenlik gibi birçok alanı tehdit edebilecek konuma geldiği için temel bir bilişim suçudur. Bu konunun önemine binaen 5237 sayılı TCK'nin243. maddesinde bilişim sistemine girme ya da kalma suçu, TCK'nin Onuncu Bölümü'nde Bilişim Alanında Suçlar başlığı altında anılan kanunun 243. maddesinde Bilişim Sistemine Girme başlığı ile yer verilmiştir. Bu hükme göre; "*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir*. (*TCK m.243/1)*

Türk Ceza Kanunu'nun 243. maddesinin birinci fıkrasına 24.03.2016 tarihinde 6698 sayılı kanunun 30. maddesinde yapılan değişiklikle; "*bilişim sisteminin tamamına veya bir kısmına hukuka aykırı olarak girmek veya orada kalmaya devam etme,"* suç olarak kabul edilmektedir. Böylelikle suçun işlenebilmesi için bilişim sisteminin tamamına ya da bir kısmına girilmesi veya orada kalmaya devam edilmesi seçimlik hareketleri aranmış ve böylelikle; bilişim sistemlerinin korunması sağlanmak istenmiştir. Bu düzenleme ile bir fiilin suç teşkil etmesi için hem bilişim sistemine girme hem de orada kalmaya devam etme fiillerinin bir arada bulunması koşulu arandığı için hükmün uygulanması konusunda doktrinde yaşanan tartışmalara da son verilmiştir.[140]

Günümüzde teknolojik gelişmelerin sürekli ivme kazanması sonucu, internetin ve elektronik araçların, iletişimde öncü bir rol üstlendiği görülmektedir. Bu bağlamda bilgisayar ve mobil cihazların belleğinde bulunan kişisel verilerin korunması, özel hayatın gizliliği açısından da hayati önem taşımaktadır. Bu nedenle Anayasamızın 20. maddesinde öngörülen *"konut dokunulmazlığı"* ve *"özel hayatın gizliliği"*nin korunmasında olduğu gibi Anayasamızın 22. maddesinde yer alan "*haberleşme hürriyeti"* de bilişim

[140] Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri,* 202.

sistemlerinin kullanımı yönünden fevkalade önem taşımaktadır. Modern dünyada; haberleşmenin ve iletişimin, mobil araçlar ile sağlanması, bu araçların bağlantılarındaki gizliliğinin korunması sorununu gündeme getirmiştir. Bu noktada; bir kişinin bilgisayarı ya da cep telefonundaki verilerin, sistem sahibinin rızası olmadan üçüncü kişiler tarafından kullanılmaması hem haberleşme özgürlüğü hem de özel hayatın gizliliği hakkı yönünden önemlidir. Aksi takdirde bilişim sistemine yetkisiz kişilerin erişmesi ve bu sistem üzerinde egemenlik kurması, sistem sahipleri ile kullanıcılarının, mağduriyetine neden olacaktır. Bu nedenle; bilişim sistemine girme ya da orada kalma suçu, diğer suçların işlenmesine de zemin hazırlamaktadır.[141] Sözgelimi, yetkin olmayan bir kişinin, başkasına ait sosyal medya hesap şifresini izinsiz olarak kullanması da haberleşme özgürlüğü ve özel hayatın gizliliği haklarının ihlaline yol açabilir[142].

Yargı Reformu Strateji Belgesi'nde yer alan İnsan Hakları Eylem Planı'nda *"Makul Sürede Yargılanma Hakkının Güçlendirilmesi"* başlığı altında; *"Bilişim alanında işlenen suçlar ile dolandırıcılık suçları başta olmak üzere soruşturma aşamasında ortaya çıkan yetki uyuşmazlıklarının hızlı bir şekilde sonuçlandırılması amacıyla gerekli tedbirler alınacaktır."* denilerek, bilişim suçları kaynaklı uyuşmazlıkların hızlı bir şekilde sonuçlanması için gereken tedbirlerin alınacağı ifade edilmiştir.[143] 30.11.2021 tarihinde R.G'de yayımlanan HSK kararı ile ihtisas mahkemelerine "bilişim ihtisas mahkemeleri" eklenmiştir. Böylece bilişim suçlarına ilişkin olarak uyuşmazlıklar, münhasıran bu suçlara yönelecek ihtisas mahkemeleri sayesinde daha hızlı ve makul bir şekilde çözüme kavuşturulacaktır. Bu nedenle kolluk personeli ve yargı mensuplarının, bilişim suçları yönünden hizmet içi eğitime tabi tutulmaları gerekmektedir. Böylece hukuki ve teknik bilgileri almak sureti ile teknolojiye uyum sağlayan bilişim hukukunda uzmanlaşan hâkimlerle birlikte "*Bilişim İhtisas Mahkemeleri*" kurulacaktır. Böylece günümüz dünyasının teknoloji ve hukukun birleşimi sonucu vazgeçilmezi konumuna gelen bilişim alanındaki suçlar ile ilgili olarak bu alandaki ihtisas

[141] Erdoğan, "Bilişim," 1375.

[142] Taşkın, "Bilişim," 335.

[143] Akaslan, "Yeni Bir İhtisas Mahkemesi Olarak Bilişim Mahkemesi." https://www.hukukihaber.net/yeni-bir-ihtisas-mahkemesi-olarak-bilisim-mahkemesimakale,8797.htm Erişim tarihi: 31 05.2021.

mahkemeleri, uyuşmazlıkları ivedi biçimde karara bağlayarak yargının iş yükünü azaltmada önemli bir rol üstlenecektir.

KAYNAKÇA

Akbulut, Berrin. "Bilişim Suçları." *Selçuk Üniversitesi Hukuk Fakültesi Dergisi 8,* no. 1-2, (Milenyum Armağanı, 2000): 545-555.

Apaydın, Cengiz. "Bilişim Sistemine Girme Suçu." *Türkiye Adalet Akademisi Dergisi* 7, no. 24 (Ocak, 2016): 245-308.

Apaydın, Cengiz. *Bilişim Suçları ve Bilişim Ceza Hukuku*. İstanbul: Acar Matbaacılık, 2017.

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

Atasoy, Fahri. "Kültürler Üzerinde Bilişim Devriminin Etkileri." *Modern Türklük Araştırmaları Dergisi 4,* no. 2, (2007): 163-177.

Avşar, B. Zakir ve Gürsel Öngören. *Bilişim Hukuku*. İstanbul: Türkiye Bankalar Birliği, 2010.

Boss, Richard, W. "Intranet andExtranet", *PLA TechNotes, American Library Association*, (2010): 1-4.

Çetin, Sefa, Muhammed. "Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu (TCK m. 243)," *Türkiye Adalet Akademisi Dergisi* 12, no. 45, (Ocak, 2021): 1-28.

Doğan, Koray. "Bilişim Suçları ve Yeni Türk Ceza Kanunu," *Hukuk ve Adalet Eleştirel Hukuk Dergisi,* no. 6-7, (2005): 290-319.

Dönmezer, Sulhi ve Sahir Erman. *Nazari ve Tatbiki Ceza Hukuku II.* İstanbul: Beta Yayıncılık, 1997.

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku.* 4. Baskı. Ankara: Seçkin Yayıncılık, 2014.

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

Ekici, Şahin, Meral ve Irmak Koruculu. "Bilişim Sistemine Girme Suçu, Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme." *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 21,* (Özel Sayı, 2019): 585-626.

Erdağ, Ali, İhsan. "Bilişim Alanında Suçlar (Türk ve Alman Hukukunda)." *Gazi Üniversitesi Hukuk Fakültesi Dergisi 14,* no. 2, (2010): 275-303.

Erdoğan, Yavuz, "Bilişim Sistemine Girme ve Kalma Suçu." *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 12*, (Özel Sayı 2012): 1363-1434.

Gezer, Sırma, Özge ve Yasemin Filiz Saygılar Kırıt. "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, (TCK m.245)," *Fasikül Hukuk Dergisi 11*, no. 111, (Şubat 2019): 429-438.

Gönen, Serkan, Halil İbrahim Ulus ve Ercan Nurcan Yılmaz. "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme," Bilişim *Teknolojileri Dergisi 9,* no. 3, (2016): 229-236.

Hakeri, Hakan. "Verileri Hukuka Aykırı Olarak Verme Suçu." *Tıbbi Müdahaleden Kaynaklanan Hukuki Sorumluluk Sempozyumu*, 16-17 Ocak 2009, Mersin Barosu Yayını, (2009): 126-131.

İhtiyaroğlu, Uğur. "Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi." *Hacettepe Üniversitesi Hukuk Fakültesi Dergisi*, (2020): 406-440.

Karagülmez, Ali. *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri.* 5. Baskı, Ankara: Seçkin Yayıncılık, 2014.

Karakehya, Hakan. "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu." *Türkiye Barolar Birliği Dergisi* 81, (2009): 1-24.

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

Koca, Mahmut ve İlhan Üzülmez. *Türk Ceza Hukuku Özel Hükümler.* 4. Baskı, Ankara: Adalet Yayınevi, 2017.

Koçak, Hüseyin ve Ali Nazmi Dandin. "Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri." *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi 19,* no. 1, (2017): 137-152.

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

Mahmutoğlu, Fatih, Selami. "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi." *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 71,* no. 1, (2013): 855-889.

Malkoç, İsmail, *Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu II.* Ankara: Malkoç Kitabevi, 2007.

Özbek, Veli, Özer, Koray Doğan Pınar Bacaksız ve İlker Tepe. *Türk Ceza Hukuku Özel Hükümler.* 11. Baskı, Ankara: Seçkin Yayınevi, 2017.

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

Soyaslan, Doğan. *Ceza Hukuku Özel Hükümler.* 11. Baskı, Ankara: Adalet Yayınevi, 2016.

Suphan, Olcay. "Konut Dokunulmazlığı Hakkı ve Konut Dokunulmazlığının İhlali Suçu." *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 6,* no. 1 (Bahar 2019): 226-266.

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

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

Tezcan, Durmuş, Mustafa Ruhan Erdem ve Rifat Murat Önok. *Teorik ve Pratik Ceza Özel Hukuku.* 17. Baskı, Ankara: Seçkin Yayınevi, 2019.

Yazıcıoğlu, Yılmaz. "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi." *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 2,* no. 2, (2005): 401-409.

Yenidünya, Caner ve Olgun Değirmenci. *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.* İstanbul: Legal Yayınevi, 2003.

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

Yılmaz, Sacit. *Türk Ceza Hukuku Sisteminde Siber Suçlar*. Ankara: Adalet Yayınevi, 2016.

Yılmaz, Zahit ve Özge Apiş. "Karşılıksız Yararlanma Suçu (TCK m.163)." *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 19*, no. 2, (2013): 1749-1779.