Av. Ahmet Alper AYDIN

# TÜRK CEZA HUKUKUNDA
# BİLİŞİM SİSTEMİNE GİRME SUÇU

**Av. Ahmet Alper AYDIN**

# TÜRK CEZA HUKUKUNDA

# BİLİŞİM SİSTEMİNE GİRME SUÇU

**ADALET YAYINEVİ**
**Ankara - 2025**

**ADALET BASIM YAYIM DAĞITIM SAN. ve TİC. LTD. ŞTİ.**

**Türk Ceza Hukukunda Bilişim Sistemine Girme Suçu**
Ahmet Alper Aydın

Hukuk Yayınları Dizisi – 3983

Birinci Baskı : Ocak, 2025

ISBN : 978 – 625 – 377 – 011 – 2

**ADALET YAYINEVİ**

*Merkez*
Strazburg Caddesi No: 10/B Sıhhiye-Ankara
Tel : (0312) 231 17 00
Fax : (0312) 231 17 10

*İstanbul Şube*
Mustafa Kemal Caddesi No: 60/C
(Anadolu Adliyesi Karşısı) Kartal-İstanbul
Tel : (0216) 305 72 81

*Dağıtım*
Strazburg Caddesi No: 17/B Sıhhiye-Ankara

*Bursa Şube*
Bursa Adliye Sarayı Zemin Kat Bursa

: adalet.com.tr – adaletyayinevi.com
: adalety@adaletyayinevi.com
: facebook.com/adaletyayinevi
: twitter.com/adaletyayinevi

*Sayfa Tasarımı:*
Nimet Yıldız

*Kapak Tasarımı:*
Yasin Özbudak

*Baskı:*
ADA Matbaacılık Yayıncılık San. Tic. Ltd. Şti.
Ostim OSB Mah. 1578. Cadde No: 21 Yenimahalle / Ankara
Tel: (0312) 385 54 10
Sertifika No: 44093

# ÖNSÖZ

Galatasaray Üniversitesi Kamu Hukuku Tezli Yüksek Programında hazırladığım aynı adlı yüksek lisans tezime dayanan bu çalışmada Türk Ceza Kanunu'nun 243. maddesinde düzenlenen bilişim sistemine girme suçu ele alınmıştır. Çalışmamın hukuk literatürü için faydalı olmasını dilerim.

Gerek konu belirleme gerekse tezin yazım sürecinin her aşamasında yanımda olarak benden hiçbir zaman desteğini esirgemeyen değerli danışmanım Prof. Dr. E. Eylem AKSOY RETORNAZ'a en içten teşekkürlerimi sunarım. Prof Dr. Pınar MEMİŞ KARTAL ve Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK'e ise tez jürime katılma nezaketini gösterdikleri ve verdikleri geri bildirimlerle çalışmama sundukları katkılar için minnettarım.

Yüksek lisans tezimin kitaplaştırılma sürecinde verdikleri destek ve sarf ettikleri emekler için başta Hakan Karaaslan, Nimet Yıldız ve Yasin Özbudak olmak üzere tüm Adalet Yayınevi ailesine teşekkür ederim.

Beraber çalıştığımız süreçte bana her türlü desteği gösteren kıymetli mesai arkadaşlarım Av. Açelya ÇAVDARLI'ya, Av. Aslı KOÇAK KALDIRIM'a ve Av. Helin Dilar ÖNÜR'e şükranlarımı sunarım. Tezimi baştan sona okuyarak katkılar sunan sevgili Mehmet Emre KANAT'a da ayrıca teşekkür ederim. Benim için çok stresli ve zorlu geçen bu süreçte sıklıkla başlarını ağrıttığım değerli dostlarım Mahmut YATI, Mustafa YILDIZ ve Sencer AYDEMİR'e ise gösterdikleri dostluk ve güzel muhabbetleri için minnettarım.

Gösterdikleri sevgi, emek ve özveri ile bugün olduğum insan olabilmemi sağlayan sevgili annem Mine AYDIN ve babam Selami AYDIN'a ne kadar teşekkür etsem yetersiz kalır. Sevgili kardeşim Mehmet Eren AYDIN'a ise dünyanın en iyi kardeşi olarak her zaman yanımda olduğu için minnettarım. Sevgili eşim ve yol arkadaşım Ayşenur Kanat AYDIN'a ise her zaman yanımda olduğu ve hayatı benim için anlamlı kıldığı için teşekkür etmek isterim.

Ekim 2024, İstanbul

**Ahmet Alper AYDIN**

# ÖZET

Bu çalışmanın konusu, 5237 sayılı Türk Ceza Kanunu'nun 243. maddesinde düzenlenen bilişim sistemine girme suçudur. Maddenin ilk fıkrasında suçun basit hali, ikince fıkrasında daha az cezayı gerektiren hali, üçüncü fıkrasında ise neticesi sebebiyle ağırlaşmış hali düzenlenmiştir. Bilişim suçlarının anlaşılması ve somut olaylarda adaletli bir karar verilebilmesi için suça konu bilişim sistemlerinin ve bu sistemlerin unsurlarının tanımlanması hayati bir öneme sahiptir. Bu nedenle çalışmamızın bilgisayar, bilişim sistemi, veri ve internet kavramları incelenmiştir. Bu kavramların teknik özelliklerine değinilmiş; ardından doktrinde ve mevzuatta yapılan tanımlar incelenmiştir. Bilişim suçlarının konusu ya da araçları olarak ortaya çıkan bu kavramların uygulamadaki durumunun daha iyi anlaşılabilmesi için Yargıtay kararlarına da bu bölümde yer verilmiştir. Yine bu bölümde ceza hukuku için yeni bir kavram olarak sayılabilecek bilişim suçu kavramının üzerinde durulmuştur. İlk olarak bu suçların adlandırılması konusunda uluslararası literatürde ve ülkemiz doktrinindeki farklı yaklaşımlar; ardından ise yapılan tanımlar ve sınıflandırmalar incelenmiştir.

Sonraki bölümde ise bilişim ve bilişim suçlarının tarihi gelişiminin incelenmesi amaçlanmıştır. İlk olarak bilgisayarın da ana vatanı olan Amerika'da ortaya çıkan bilişim suçlarının gelişimi ve bu suçların engellenmesi için ülkeler tarafından yapılan çalışmalara değinilmiştir. Ardından bilişim suçları ile ilgili olarak hazırlanan en önemli ve geniş kapsamlı uluslararası belge olan Avrupa Konseyi Siber Suç Sözleşmesi'nin hazırlanma süreci ve incelemekte olduğumuz suç ile ilgili maddelerinin üzerinde durulmuştur. Devamında ise bilişim suçlarının ülkemiz mevzuatlarına girişi için yapılan çalışmalar ile 765 sayılı TCK'ya eklenen bilişim suçları ile ilgili maddelerin incelemesi yapılmıştır. Türk ceza reformu kapsamında yeni bir ceza kanunu yapmaya yönelik hazırlanan tasarılar ile bunlarda yer alan bilişim suçlarına ilişkin maddeler de yine çalışmamızda yer almıştır. Son olarak bilişim sistemine girme suçunun ülkemizde ilk defa düzenlendiği 5237 sayılı TCK'nın hazırlanış süreci ve bu kanunda yapılan değişiklikler üzerinde durulmuştur.

Kavramlar ile ilgili temel bilgiler ve tarihi arka planın okuyucuya aktarılması üzerine TCK m. 243'te düzenlenen bilişim sistemine girme suçu incelenmesine başlanmıştır. Bilişim sistemine girme suçu ile korunmak istenen hukuki değer ile ilgili doktrinde farklı görüşler dile getirilmiştir. Malvarlığı, özel hayatının gizliliği, haberleşme özgürlüğü, kişisel veriler ve sistemin güvenliği gibi değerlerin birinin ya da birkaçının birlikte korunmasının amaçlandığı yazarlarca öne sürülmüştür. Bize göre ise bu suç ile korunmak istenen hukuki değer yalnızca bilişim sistemlerinin güvenliğidir. Kanun koyucu sayılan diğer menfaatleri TCK'da yer alan farklı suçlarla korumuştur. TCK m. 243'üç basit hali ile korunmak istenen değer bilişim sisteminin güvenliğidir. Üçüncü fıkradaki niteliği sebebiyle ağırlaşmış halde ise korunmak istenen değer sistemde bulunan verilerdir.

Her gerçek kişi bu suçun faili olabilecektir. Tüzel kişiler ise ceza hukuku anlamında fail olamayacaklardır. Bununla birlikte suçun işlenmesi ile menfaat temin eden tüzel kişiler hakkında TCK m. 60'da öngörülen güvenlik tedbirlerine hükmedilebilecektir. Her ne kadar kanunda bilişim suçlarının işlenebilmesi için özel bir meslek ya da statü sahibi olmak gibi bir şart aranmasa da bu suçların genellikle "hacker" olarak adlandırılan bilişim korsanlarınca işlendiği görülmektedir. Suçun mağduru ise sistem üzerinde hak sahibi olan ve sisteme doğrudan erişim yetkisine sahip kişidir. Sistem sahibi tarafından hukuka uygun bir şekilde sisteme erişim yetkisi verilmiş kişiler de bu suçun mağduru olabilirler. Kuşkusuz ki gerçek kişiler bu suçun mağduru olabileceklerdir. Tüzel kişilerin durumu ise tartışmalıdır. Kimi yazarlar tüzel kişilerin mağdur olamayacaklarını, ancak suçtan zarar gören olabileceklerini savunmaktadır. Bizim de katıldığımız yazarlar ise TCK'da tüzel kişilerin mağdur olmalarına engel bir hüküm olmadığını öne sürerek; bunların da mağdur olabileceklerini savunmaktadır. Suçun niteliğine uygun düştüğü sürece tüzel kişiler de bilişim sistemine girme suçunun mağduru olabileceklerdir.

Bilişim sistemine girme suçunun konusu bilişim sistemleridir. Genel amaçlı olarak kullanılabilen bu sistemler verileri işleyebilir, birbirleri arasında aktarabilir ve depolayabilirler. Barkod okuyucular, beyaz eşyalar ve kahve otomatları gibi sadece belli bir işi yapabilen cihazlar bilişim sistemi olarak kabul edilmemektedirler. Bununla birlikte son yıllarda ortaya çıkan nesnelerin interneti ile diğer nesneler ile bilişim sistemlerine veri gönderebilen ya da bunlardan veri alabilen beyaz eşyalar ya da akıllı saatler gibi giyilebilir teknoloji ürünleri bilişim sistemi olarak kabul edilmelidir. Gü-

nümüzde artık internete bağlanabilen ve birçok bankacılık işleminin yapılabildiği ATM'ler ise bilişim sistemi sayılmaktadır. Bilgisayarlar, akıllı telefonlar, tabletler en yaygın bilişim sistemleridirler. Belli bir donanıma bağlı olmayan ve uzaktan erişilebilen internet siteleri, sosyal medya uygulamaları, e-posta adresleri, online veri tabanları ve video oyunu oynama hizmeti veren platformlar da yine bilişim sistemi olarak kabul edilmektedir. Son yıllarda insanlığın hayatına giren bulut bilişim sunucuları ile nesnelerin interneti ile çalışan akıllı sistemler de yine bilişim sistemi olarak kabul edilmektedirler. TCK m. 243'te suçun bilişim sisteminin tamamına ya da bir kısmına karşı işlenebileceği düzenlenmiştir; bu nedenle sistemin belli bir parçası ya da sisteme bağlı bir aygıt da bu suçun konusu olabilir. Örneğin bilişim sisteminin içerisinde bulunan belli bir klasör ya da sisteme bağlanmış bir harici bellek de suçun konusu olabilir. Suçun daha az cezayı gerektiren halinin konusu bedeli karşılığı yararlanılabilen bilişim sistemleridir. Suçun netice itibariyle ağırlaşan halinin konusu ise sistemin içerisindeki verilerdir.

Failin bilişim sistemine girme veya sistemde kalmaya devam etme hareketlerinden birini yapması ile suç işlenmiş olacaktır. Girme eylemi fiziksel olarak sisteme temas edilerek icra edilebileceği gibi; internet ağları ya da kablolar yardımıyla uzaktan da icra edilebilecektir. Girme eyleminin suç olarak kabul edilebilmesi için sistemin özel olarak korunmasına gerek yoktur; girişin hukuka aykırı olması yeterlidir. Bir başka failin sisteme girme eyleminin hukuken geçerli bir hak ya da rızaya dayanmaması gerekmektedir. Herkesin erişimine açık bir sisteme girilmesi halinde suç oluşmayacaktır. Sistemin fiziksel yapısına değil çalışan sanal/dijital alana girilmesi gerekmektedir. Fail bilişim sisteminin düğmesine basarak bu suçu işleyebileceği gibi farklı yöntemler ve yazılımlar da kullanabilecektir. Bilişim suçlarını işlemeyi meslek haline getirmiş hackerlar tarafından bu suçların işlenebilmesi için çeşitli yazılımlar kullanılabilmektedir. Tarama yöntemi ile sistemin açıklarını tespit eden bilişim korsanları; virüsler, solucanlar, Truva atları gibi zararlı yazılımlar ile sisteme girmeye çalışmaktadır. Sosyal mühendislik ve oltalama gibi psikolojik manipülasyon yöntemleri de yine bilişim korsanlarınca sıkça kullanılmaktadır. Özellikle son yıllarda geliştirilen Pegasus yazılımı gibi programlarla sistem sahiplerine sadece dosya gönderilerek hedef bilişim sistemine girilebildiği görülmektedir. Kalma eyleminin icra edilebilmesi için ilk olarak failin sisteme girmiş olması gerekmektedir. Fail sisteme hukuka uygun bir şekilde girmiş olmasına rağmen hukuka uygunluk sebebi ortada kalkmış olabilir. Bu durumu fark eden

fail hemen sistemden çıkmazsa sistemde kalmaya devam etme fiilini işlemiş olacaktır. Hata sonucu sisteme girdiği sistemden hatasını fark etmesine rağmen çıkmayan fail de bu suçu işlemiş olacaktır.

Suçun işlenmesi için özel bir neticenin ya da zararın meydana gelmesin gerek yoktur. Fail sisteme girdiği veya kalmaya devam ettiği anda suç işlenmiş olacaktır. Suçun neticesi sebebiyle ağırlaşmış hali için ise kanun koyucu verilere zarar gelmesini netice olarak düzenlemiştir. Bilişim sistemine girme suçu bakımından teşebbüs mümkündür. Sisteme girmek için icrai hareketlere başlayan fail elinde olmayan nedenlerle sisteme giremezse teşebbüs hükümlerine göre cezalandırılacaktır. Kalmaya devam etme eylemi bakımından ise teşebbüs mümkündür. Teşebbüsün mümkün olduğu hallerde TCK m. 36'da düzenlenen gönüllü vazgeçme hükümleri de uygulanacaktır. Gönüllü olarak suçun icra hareketlerini yarıda bırakan faile sadece o zamana kadar işlediği suçlardan dolayı ceza verilecektir.

Bilişim sistemine girme suçu sadece kasten işlenebilmektedir. Taksirle ya da hata sonucu bir sisteme girilmesi halinde faile ceza verilmeyecektir. Suçun oluşumu ve failin cezalandırılması açısından failin amacının bir önemi yoktur. Failin kusurluluğunu ortadan kaldıran hallerin varlığında ise kusur yeteneği mevcut olmayacağı için suç da oluşmayacaktır. TCK m. 243/3'te düzenlenen suçun işlenmesi için ise fail kasten bilişim sistemine girmiş olmalı ve taksirli bir hareketle sistemdeki verilere zarar vermelidir.

İncelemekte olduğumuz suçu düzenleyen maddedeki "*hukuka aykırı olarak*" ifadesinin anlamı doktrinde tartışılmaktadır. Kimi yazarlar kanun koyucunun bu tercihi ile hukuka aykırılık bilincini de suçun bir unsuru olarak kabul ettiğini savunmaktadır. Bizim katıldığımız görüşe göre ise kanun koyucunun buradaki amacı suçun işlenmesi sırasında ortaya çıkabilecek hukuka uygunluk nedenlerine dikkat çekmektir. Önemli olan hukuka uygunluk halinin bulunup bulunmadığıdır. Failin özel olarak hukuka aykırılık bilinciyle hareket etmiyor olsa bile suçun diğer unsurları gerçekleştiği takdirde fail cezalandırılacaktır. Bir kanun hükmünün icrası kapsamında bir başkasına ait bilişim sistemine giren kişi cezalandırılmayacaktır. Bu konuda verilecek başlıca örnekler bilgisayar kütüklerinde arama ve iletişimin denetlenmesi tedbirleridir. Bilişim sistemini bir suçu önlemek için meşru müdafaa kapsamında işleyen fail de cezalandırılmayacaktır. Bir hakkın kullanılması kapsamında bilişim sistemine giren fail de cezalandırılmayacaktır. Örneğin abonelik sözleşmesi kişilere başkalarına ait ilişim sistemlerine erişme hakkı verebilmektedir. Sistem sahibinin verdiği rızaya

uygun bir şekilde sisteme giren kişi de cezalandırılmayacaktır. Rıza açık bir şekilde verilebileceği gibi örtülü olarak da verilmiş olabilir. Sistem sahibinden aldığı rıza ile sisteme giren bir kimsenin üçüncü kişilere vereceği rıza geçerli olmayacaktır. Rıza belli bir şarta bağlı olarak verilebileceği gibi; belli bir amacın ifasına yönelik olarak da verilebilecektir. Ayrıca belli bir süreliğine rıza verilmesi de mümkündür. Sızma testleri ile sistemin güvenliğini test eden beyaz şapkalı hackerların eylemleri rıza kapsamında olacağı için suç oluşmayacaktır. Çalışanlarına bilgisayar tahsis eden kurumda bunları kullanabilmeleri için çalışanlarına rıza göstermiştir. Kurumların, çalışanlarını denetlemek amacıyla bilgisayarlar ve mail adreslerine erişmelerinin suç olup olmadığı da önemli bir konudur. AİHM ve Anayasa Mahkemesi kararlarına göre işverenlerin denetim yapmadan önce bu denetimlerin kapsamı ve sınırları hakkında çalışanlarını bilgilendirmeleri ve onaylarını almaları gerekmektedir. Aksi halde yapılan denetim bilişim sistemine girme suçunu oluşturacaktır.

Bilişim sistemine girme suçunun bedeli karşılığı yararlanılabilen sistemlere karşı işlenmesi halinde verilecek ceza azaltılacaktır. Burada kastedilen internet kafeler gibi bilişim sistemlerinin kiralandığı mekanlar değildir. Suçun bu halinin ulaşması için bilişim sistemini sanal yapısı üzerinden sunulan bir hizmet söz konusu olmalıdır. Üyelerine üret karşılığı çeşitli hizmet sunan internet siteleri, video oyunu oynana platformları ve kullandığın kadar öde sistemi ile çalışan uygulamalar bu sistemlere örnek olarak gösterilebilir. İnternet hizmetinin yetkisiz bir şekilde kullanılması da bu fıkra kapsamında değerlendirilecektir. IPTV ve WEBTV gibi internet tabanlı sunulan şifreli yayınların izlenmesi de yine TCK m. 243/2 kapsamındadır. Telefon ve manyetik hatlar ile sunulan şifreli yayın hizmeti ile otomatların bedeli ödenmeksizin kullanması ise TCK m. 163'te düzenlenen karşılıksız yararlanma suçunu oluşturacaktır. Bilişim sistemine girme suçunun bir terör örgütünün faaliyetleri çerçevesinde işlenmesi halinde verilecek ceza artırılacaktır. Ayrıca kimi yazarlar kamu kurumlarına ait ve devletin güvenliği ile ilgili sistemler ile özel güvenlik önlemleri ile korunan sistemlere karşı işlenen suçların daha ağır bir şekilde cezalandırılmasını savunmaktadır. Bilişim sistemine girme suçunun işlenmesi nedeniyle sistemdeki verilerin değişmesi ya da yok olması halinde ise TCK m. 243 uygulanacaktır. Burada bilerek ve isteyerek bilişim sistemin giren fail istemeden sistemdeki verilere zarar vermektedir. Kasten verilere zarar veren fail ise TCK m. 244 gereğince cezalandırılacaktır. Kanunun gerekçesinde veri sistemdeki tüm soyut unsurlar olarak tanımlanmıştır.

Bilişim sistemine girme suçu bir başka suçun ağırlaştırıcı sebebi ya da unsuru olarak işlenmişse bileşik suç söz konusudur. Örneğin bilişim sistemleri kullanılması yoluyla hırsızlık (TCK m. 142/2-e) ve bilişim sisteminin araç olarak kullanılması yoluyla dolandırıcılık (TCK m. 158/1-f) suçlarında fail asıl hedeflediği suçun unsuru olarak TCK m. 243'te düzenlenen suçu işlemektedir. Bu durumda faile bilişim sistemine girme suçundan dolayı ceza verilmeyecektir. Bilişim sistemine girme suçunun aynı kişiye karşı farklı zamanlarda birden fazla kere işlenmesi halinde zincirleme suç söz konusu olacaktır. Suçun tek fiille birden fazla sisteme karşı işlenmesi halinde de yine aynı durum söz konusu olacaktır. Burada tek bir ceza verilecek ve söz konusu ceza TCK m. 43'e göre artırılacaktır. Tek bir fiil ile birden fazla suçun işlenmesi halinde faile yalnızca en ağır suç için ceza verilecektir. Bilişim sistemine girme suçunu işleyen kişi kimi zaman aynı fiille haberleşmenin gizliliğini ihlal, özel hayatın gizliliğini ihlal veya kişisel verilerin ele geçirilmesi suçlarını işleyebilmektedir. Eğer bu suçların işlendiği fiil aynıysa faile yalnızca tek bir ceza verilecektir. Buna rağmen her suça sebebiyet veren fiil farklıysa fail her suç bakımından ayrı ayrı cezalandırılmalıdır. Benzer bir tartışma TCK m. 244'te düzenlenen suçlar bakımından da söz konusudur. Fail TCK m. 244'teki suçu işlemek için bilişim sistemine girme suçunu bir araç suç olarak işlemişse TCK m. 243 gereğince cezalandırılmayacaktır. Failin TCK m. 244'teki suçu işlemesi için bilişim sistemine girmesi kaçınılmaz ise sadece bu madde gereğince ceza verilmelidir. Bununla birlikte zorunda olmamasına rağmen bilişim sistemine giren faile ayrıca TCK m. 243 gereğince de ceza verilecektir. Kimi zaman bilişim sistemine girme suçunu işlemek isteyen fail, işini kolaylaştırmak amacıyla TCK m. 245A'da düzenlenen yasak cihaz ve programlar suçunu işleyebilmektedir. Burada faile hem TCK m. 243 hem de TCK m. 245A gereğince ceza verilmelidir.

Bilişim sistemine girme suçu tek kişi tarafından işlenebileceği gibi; birden fazla kişinin de bu suçu birlikte işlemesi mümkündür. Dolaylı faillik, yardım etme ve azmettirmeye ilişkin hükümlerin de bu suçu uygulanması önünde herhangi bir engel yoktur. Bilişim sistemine girme suçunu işleyen fail, suçun işlendiği yerdeki asliye ceza mahkemesinde yargılanacaktır. 2021 yılından itibaren iki veya daha fazla asliye ceza mahkemesi olan yerlerde belli mahkemeler bilişim alanında ihtisas mahkemesi olarak çalışmaya başlamıştır.

# İÇİNDEKİLER

# KISALTMALAR

| | | |
|---|---|---|
| **ABD.** | **:** | Amerika Birleşik Devletleri |
| **a.g.e.** | **:** | Adı Geçen Eser |
| **a.g.m.** | **:** | Adı Geçen Makale |
| **AİHM** | **:** | Avrupa İnsan Hakları Mahkemesi |
| **AİHS** | **:** | Avrupa İnsan Hakları Sözleşmesi |
| **Alm.** | **:** | Almanca |
| **AKSSS** | **:** | Avrupa Konseyi Siber Suç Sözleşmesi |
| **AYM** | **:** | Anayasa Mahkemesi |
| **C.** | **:** | Cilt |
| **CD.** | **:** | Ceza Dairesi |
| **Der.** | **:** | Derleyen |
| **CMK** | **:** | Ceza Muhakemeleri Kanunu |
| **DEÜHFD** | **:** | Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi |
| **E.T.** | **:** | Erişim Tarihi |
| **E.** | **:** | Esas Numarası |
| **Fra.** | **:** | Fransızca |
| **FSEK** | **:** | Fikir ve Sanat Eserleri Kanunu |
| **İÜHFM** | **:** | İstanbul Üniversitesi Hukuk Fakültesi Mecmuası |
| **İng.** | **:** | İngilizce |
| **K.** | **:** | Karar Numarası |
| **PVSK** | **:** | Polis Vazife Ve Salâhiyet Kanunu |
| **s.** | **:** | Sayfa |
| **S.** | **:** | Sayı |
| **T.** | **:** | Tarih |

**TBMM** **:** Türkiye Büyük Millet Meclisi

**TCK** **:** Türk Ceza Kanunu

**TDK** **:** Türk Dil Kurumu

**TÜİK** **:** Türkiye İstatistik Kurumu

**Yar.** **:** Yargıtay

**YCGK** **:** Yargıtay Ceza Genel Kurulu

YHGK : Yargıtay Hukuk Genel Kurulu

# GİRİŞ

1946 yılında geliştirilen ve tarihteki ilk bilgisayar olarak kabul edilen ENIAC[1] ile hayatımıza giren bilişim sistemleri; günümüze değin geçen sürede çok hızlı bir şekilde değişmiş ve gelişmiştir. Bilişim teknolojileri profesyonel iş hayatından, eğitime; eğlenceden, alışverişe kadar birçok alanda hayatın vazgeçilmez bir parçası olmayı başarmıştır. Öyle ki TÜİK verilerine göre 2021 yılında Türkiye'deki hanelerin %80,5'i bilişim sistemleri ve internet düzenli olarak kullanmaktadır[2]. Hayatın her alanına sirayet eden bilişim sistemleri aynı zamanda yeni suç tiplerinin ortaya çıkması ve işlenmesi için uygun bir ortam olmuştur.

İlk defa altmışlı yıllarda Amerika'da ortaya çıkan[3] bilişim suçları; kişisel bilgisayarlar ve internetin yaygınlaşarak evlerde kullanılmaya başlandığı doksanlı yıllara gelinmesiyle birlikte yaygınlaşmıştır[4]. Bilişim suçlarının işlenme şekillerinin ve sayılarının arttığı bu yıllarda devletler de bu suçlar ile ilgili cezai düzenlemeleri yürürlüğe koymaya başlamıştır[5]. Yine bu yıllarda uluslararası örgütler tarafından da bilişim suçları üzerine çeşitli çalışmalar yapılmış; 2001 yılında ise bilişim suçları alanındaki ilk ve en önemli uluslararası belge olarak kabul edilen Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS) hazırlanarak imzaya açılmıştır[6].

---

1 Ahmet Caner Yenidünya/Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003 s. 13-14.

2 TÜİK, **2021 Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması** https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437 (E.T. 11.04.2022)

3 Emin Doğan Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Ankara: Doruk Yayınları, 1992 s. 25.

4 Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, **8. Baskı,** Ankara: Seçkin Yayıncılık, 2020 s. 93-94.

5 Levent Kurt, **Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara: Seçkin Yayınevi, 2005 s. 115.

6 Murat Önok, "*Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği*", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Prof. Dr. Nur Centel'e Armağan**, C.9, S. 2, 2013 s. 1241.

Ülkemizde ise 1991 yılında 765 sayılı TCK'da yapılan değişiklikle birlikte bilişim suçları ceza kanunumuza girmiştir[7]. Ancak bu değişiklik ile kanuna eklenen maddeler arasında bu çalışmanın konusu olan bilişim sistemine girme suçunu düzenleyen bir madde bulunmamaktaydı. Bilişim sistemine girme eylem ilk defa 5237 sayılı TCK'nın 243. maddesinde suç olarak düzenlenmiştir[8]. 2016 yılında ise TCK m. 243'te çeşitli değişiklikler yapılmıştır. Maddenin güncel hali şu şekildedir:

*Bilişim sistemine girme*

**Madde 243-** "*(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.*

*(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.*

*(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.*

*(4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*"

Maddenin ilk fıkrası bilişim sistemine girme suçunun basit halini, ikinci fıkrası cezanın azaltılmasını gerektiren halini, üçüncü fıkrası ise suçun ortaya çıkan netice nedeniyle ağırlaşan halini düzenlemektedir. Maddeye 2016 yılında eklenen dördüncü fıkrada ise "*veri nakillerini izleme suçu*" düzenlenmiştir. Bu suç her ne kadar TCK m. 243 içerisinde düzenlenmiş olsa da bilişim sistemlerine girmeksizin işlenen bir suçtur. Doktrinde de bu suçun ayrı bir maddede düzenlenmesinin daha sağlıklı olacağı ifade edilmiştir[9]. Koruduğu hukuki değer, suçun konusu ve icra edilen fiiller yönünden bilişim sistemine girme suçu ile arasında önemli farklar bulunan dördüncü fıkra bu çalışma kapsamında incelenmeyecektir.

---

7 Akbulut, **Bilişim Alanında Suçlar, 2. Baskı**, Ankara: Adalet Yayınevi s. 96-97. Kurt, **a.g.e.** s. 118-121.

8 Akbulut, **a.g.e.** s. 112. Kurt, **a.g.e.** s. 136.

9 Akbulut, **Ba.g.e. Suçlar** s. 158-159. Dülger, **a.g.e.** s. 237. Ahmet Gül, **Doğrudan-Dolaylı Bilişim Suçları**, **3. Baskı,** Ankara: Seçkin Yayıncılık, 2021 s. 91.

Çalışmamızda TCK m. 243'ün ilk üç fıkrasında düzenlenmiş olan bilişim sistemine girme suçu incelenecektir. İşlenen bir fiilin TCK'da düzenlenmiş olan suç tipinin kapsamına girip girmediğinin tipiklik unsuru yönünden değerlendirilebilmesi için ilk olarak bilişim, bilişim sistemi ve ilgili kavramların sınırlarının açık ve net bir şekilde tespit edilebilmesi gerekmektedir. Bilişim sistemleri ve bu sistemlerin bileşenlerinin tanım ve özellikleri, gelişen teknolojiyle de bağlantılı olarak, her geçen gün gelişmekte ve değişmekte; bu değişim ise aşağıda değinilecek kavramların tanımlanmasını daha da zorlaştırmaktadır[10]. Öte yandan bu kavramlara kanuni düzenlemelerle yapılacak tanımlar zaman içinde yetersiz kalacak, bu durum ise ortaya çıkan yeni suç işleme biçimlerinin kanunun kapsamı dışında kalmasına neden olacaktır[11]. Bu nedenledir ki bazı yazarlar bilişim kavramlarının tanımını yapmaktan kaçınıp özelliklerini saymakla yetinirken[12] bazı yazarlar ise teknik ayrıntı ve terimlerden arındırılmış kısa ve öz tanımlar yapmayı tercih etmiştir[13]. Suçun unsurlarının incelenmesi sırasında meydana gelebilecek olası karışıklıkların önüne geçilebilmesi maksadıyla; çalışmamızın ilk bölümünde doktrinde yapılan tanımlar yargı kararları ile birlikte bütüncül bir şekilde ele alınacaktır. Bu bölümde çoğunlukla incelemekte olduğumuz suçun konusu olacak bilgisayar ve bilişim sisteminin yanında; veri ve internet gibi suçla yakın ilişkili kavramlara da değinilecektir. Ayrıca bilişim kavramının isimlendirilmesi, tanımlanması ve sınıflandırılmasına ilişkin doktrindeki yaklaşımlara değinilmiştir.

Kavramların tanımlanmasının ardından, okuyucunun kavramların tarihi arka planına hâkim olması amacıyla, bilişim ve bilişim suçlarının tarihi gelişimine değinilecektir. Ardından ülkemizin de taraf olduğu AKSSS'nin hazırlanış süreci ile incelemekte olduğumuz suçla ilgili hükümlerinden bahsedilecektir. Akabinde ise 765 sayılı TCK döneminde bilişim suçları ile ilgili hazırlanan tasarılar ve yapılan kanun değişiklikleri ele alınacaktır. Bu sırada 5237 sayılı TCK'nın hazırlık süreci ile bu dönemde yapılan tartışmaların üzerinde durulacaktır.

Çalışmanın devamında ise suçla korunan hukuki değer doktrindeki farklı görüşler ve yargı kararları ışığında incelenecektir. Ardından suçun

---

10 Dülger, **a.g.e.** s. 58.

11 Büşra Özçelik, **Bilişim Sistemine Girme Suçu**, İstanbul: On İki Levha Yayınları: İstanbul Ceza Hukuku ve Kriminoloji Arşivi, 2021 s. 3-4.

12 Yenidünya/Değirmenci **a.g.e.** s. 31

13 Dülger, **a.g.e.** s. 64-65.

maddi unsurları, manevi unsuru ve hukuka aykırılık unsuru tek tek incelenerek bu konularda doktrinde ve yargı kararlarında belirtilen önemli hususların üzerinde durulacaktır. Yine aynı başlık altında; suçun cezasını hafifleten ve ağırlaştıran nedenler ile suçun neticesi sebebiyle ağırlaşmış hali incelenecektir. Suçların birleşmesi başlığı altında ise bilişim sistemine girme suçunun farklı suçlarla beraber işlenmesi halinde failin nasıl cezalandırılacağı sorusunun üzerinde durulacaktır. Bu kapsamda TCK'nın ilgili maddelerinde düzenlenen bileşik suç, zincirleme suç ile aynı ve farklı neviden fikri içtima hallerine ayrı ayrı değinilecek; bu hallerde hakim tarafından uygulanacak kurallar örnekler, doktrin görüşleri ve yargı kararları ile belirlenmeye çalışılacaktır. İştirak başlığı altında ise birden fazla fail olması veya faile yardım edilmesi yahut failin suça azmettirilmesi durumlarında uygulanacak hükümlerin üzerinde durulacaktır. Yaptırım bölümünde suçun basit hali ve nitelikli halleriyle neticesi sebebiyle ağırlaşmış haline verilecek ceza ve bu cezanın nasıl belirleneceği üzerinde durulacaktır. Yargılama başlığı altında ise yakın zamanda CMK'da yapılan değişiklikler de ele alınarak bilişim sistemine girme suçunun soruşturma ve kovuşturma evrelerinin nasıl yürütüleceği açıklanacaktır.

Bu çalışmada gerek suçla ilgili temel kavramlar gerekse suçun unsurlarına ilişkin tartışmalarda ilgili Yargıtay Ceza Genel Kurulu ve ceza dairesi kararlarına değinilerek uygulamadaki güncel durum da okuyucuya aktarılacaktır. Konu ile ilgisi bulunan hallerde ise Avrupa İnsan Hakları Mahkemesi ile Anayasa Mahkemesi kararlarına yer verilecektir. Yargı kararlarının yanı sıra doktrindeki farklı görüşlere de değinilerek işlenen konuların olabildiğince geniş bir perspektiften incelenmesi amaçlanmaktadır.