Hazırlayan

ANABİLİM DALI

Yüksek Lisans Tezi

2025

T.C.
ERCİYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME (TCK M. 244/1-2)

Hazırlayan
Melahat Şeyma DOĞRUOĞLU

Danışman
Doç. Dr. Ahmet Hulusi AKKAŞ

Yüksek Lisans Tezi

Nisan 2025, KAYSERİ

T.C.
ERCİYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME (TCK M. 244/1-2)

(Yüksek Lisans Tezi)

Hazırlayan
Melahat Şeyma DOĞRUOĞLU

Danışman
Doç. Dr. Ahmet Hulusi AKKAŞ

Nisan 2025, KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Melahat Şeyma DOĞRUOĞLU

T.C.

ERCİYES ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Anabilim Dalı : Kamu Hukuku

Program Adı : Tezli Yüksek Lisans

Tez Başlığı : Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (TCK m. 244/1-2)

Yukarıda bilgileri verilen tez çalışmasının a) Giriş, b) Ana bölümler ve c) Sonuç kısımlarından oluşan (Kapak, Önsöz, Özet, İçindekiler ve Kaynakça hariç) toplam 163 sayfalık kısmına ilişkin 11/04/2025 tarihinde ***Turnitin*** intihal programından aşağıda belirtilen filtreleme uygulanarak alınmış olan özgünlük raporuna göre tezin benzerlik oranı**: % 15'**tir.

Filtrelemeye **alıntılar dahil** edilmiştir. Filtrelemede **yedi (7) kelimeden daha az** örtüşme içeren metin kısımları hariç tutulmuştur.

Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Tez İntihal Raporu Uygulama Esaslarını inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına göre tez çalışmasının herhangi bir intihal içermediğini, aksinin tespit edilmesi durumunda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini bilgilerinize arz ederim. 11/04/2025

Danışman: Doç. Dr. Ahmet Hulusi AKKAŞ Öğrenci: Melahat Şeyma DOĞRUOĞLU

KILAVUZA UYGUNLUK

"Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (TCK m. 244/1-2)" başlıklı Yüksek Lisans Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Lisansüstü Tez Yazım Kılavuzuna uygun olarak hazırlanmıştır.

Hazırlayan	**Danışman**
Melahat Şeyma DOĞRUOĞLU	Doç. Dr. Ahmet Hulusi AKKAŞ

Kamu Hukuku ABD Başkanı

Prof. Dr. Cengiz GÜL

KABUL VE ONAY TUTANAĞI

Doç. Dr. Ahmet Hulusi AKKAŞ danışmanlığında **Melahat Şeyma DOĞRUOĞLU** tarafından hazırlanan **"Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme (TCK m. 244/1-2)"** adlı bu çalışma jürimiz tarafından Erciyes Üniversitesi Sosyal Bilimler Enstitüsü **Kamu Hukuku** Anabilim Dalı'nda **Yüksek Lisans Tezi** olarak kabul edilmiştir.

11/04/2025

JÜRİ:

Danışman : **Doç. Dr. Ahmet Hulusi AKKAŞ**

Üye : **Dr. Öğr. Üyesi Hüseyin ERTUĞRUL**

Üye : **Dr. Öğr. Üyesi Şenel SARSIKOĞLU**

ONAY:

Bu tezin kabulü Enstitü Yönetim Kurulu'nun …. /…./…… tarih ve …….. sayılı kararı ile onaylanmıştır.

……. /…..…../ ……..…

Prof. Dr. Atabey KILIÇ

Enstitü Müdürü

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME (TCK m. 244/1-2)

Melahat Şeyma DOĞRUOĞLU

Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü
Yüksek Lisans Tezi, Nisan 2025
Danışman: Doç. Dr. Ahmet Hulusi AKKAŞ

ÖZET

Bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme suçları günümüzde işlenme oranı giderek artan ve sadece bireyleri değil; toplumları ve devletleri etkileyebilecek nitelikte zararlara yol açabilen suçlardır. Bilişim suçlarının işlenmesinde failin anonim bir biçimde hareket edebilmesi ve dünyada internetin bulunduğu her noktaya erişim sağlama imkânına erişmesi, bilişim sistemlerinin kullanıldığı birçok alanı tehlikeye sokmakta ve bu suçlarla mücadelede uluslararası işbirliğini gerekli kılmaktadır.

Bilişim teknolojilerinin gelişim hızı bilişim suçlarıyla mücadeleye yönelik hukuksal çalışmaların teknolojik gelişmelere yetişmesini zorlaştırmakta ve kanun koyucuyu genel ve kapsayıcı bir hukuki düzenleme oluşturmaya itmektedir. Nitekim TCK m. 244'te yer alan düzenlemede de bu durum açıkça görülmektedir. Bununla beraber yapılan düzenleme doktrinde birçok tartışmaya yol açmış, yargıda birbiriyle çelişkili kararların ortaya çıkmasına zemin hazırlamış ve kanunilik ilkesinin uygulanmasını zorlaştırmıştır. Bilişim alanındaki kavramların tam olarak oturtulamaması ve bilişim suçunun tanımlanmasında yaşanan zorluklar da bu durumu pekiştirmiştir. Kanunda dijital veri mülkiyetine ilişkin bir düzenleme yapılmamıştır. Bu nedenle maddi varlığı olmadığından ceza hukukunda taşınır mal olarak değerlendirilemeyen bilişim verileri hırsızlık ve mala zarar verme suçu gibi klasik suç tipleri açısından koruma dışı kalmıştır.

Çalışmamızda bilişim alanında genel kavramlara, bilişim suçlarına ve işleniş biçimlerine yer verilmiş, daha sonrasında ise TCK m. 244/1-2'de yer alan suçların ayrıntılı olarak incelemesi yapılmıştır.

Anahtar Kelimeler: Bilişim Suçu, Veri, Sisteme Müdahale, Verilere Müdahale.

OBSTRUCTION/DISRUPTION OF THE INFORMATION SYSTEM, DESTRUCTION/MANIPULATION OF DATA (TPC art. 244/1-2)

Melahat Şeyma DOĞRUOĞLU

Erciyes University, Graduate School of Social Sciences
Master's Thesis, April 2025
Supervisor: Doç. Dr. Ahmet Hulusi AKKAŞ

ABSTRACT

Crime of blocking/disrupting/destroying or changing information technology (IT) systems and their data are increasingly being committed today and affect not only individuals but also cause severe harm to societies and states. The fact that the perpetrator can act anonymously when committing cyber crimes and has the opportunity to access every point in the world where the internet is available endangers many areas where IT systems are used and requires international cooperation in the fight against these crimes.

The speed of development of IT systems makes it difficult for legal studies to combat cyber crimes to keep up with technological developments and pushes the legislator to create more general and comprehensive legal regulation. As a matter of fact, this situation is clearly seen in the regulation in TPC art. 244. However, the regulation has led to many debates in the doctrine, paved the way for contradictory decisions in the judiciary, and made the application of the legality principle difficult. The inability to fully establish the concepts in IT field and the difficulties in defining cybercrime have also reinforced this situation. No modification on the ownership of IT data has been made in TPC art. 244. Since IT data cannot be considered as a property and that there are no regulations regarding to its legal qualification, the data become unprotected as compared with qualified crimes such as theft or damaging property.

General concepts in IT systems, cyber crimes and the ways being committed are explored in current study as the crimes defined in TPC art. 244/1-2 are examined in detail.

Keywords: Computer Crime, Data, System Intervention, Data Intervention.

İÇİNDEKİLER

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME (TCK m. 244/1-2)

İKİNCİ BÖLÜM

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

KISALTMALAR LİSTESİ

ABD : Anabilim Dalı

ABD : Amerika Birleşik Devletleri

AİHS : Avrupa İnsan Hakları Sözleşmesi

AKSSS : Avrupa Konseyi Siber Suç Sözleşmesi

ARPANET : Advanced Research Projects Authority Net

ATM : Automated Teller Machine

BAP : Bilimsel Araştırma Projeleri

Bkz : bakınız

CDA : Communications Decency Act

CGK : Ceza Genel Kurulu

CIA : Central Intelligence Agency

CMK : Ceza Muhakemesi Kanunu

COPA : Child Online Prevention Act

CPPA : Child Pornography Preventionact

CPU : Central Processing Unit

CSA : Cloud Security Alliance

DDoS : DistrubutedDenial of Service Attack

DoS : Denial Of Service

ERÜ : Erciyes Üniversitesi

HMK : Hukuk Muhakemeleri Kanunu

IC3 : Internet Crime Complaint Center

IoT : Internet of Things

ISS : İnternet servis sağlayıcıları

LAN : Local Area Network

MAN : Metropolian Area Network

NW3C : National White Collar Crime Center

ODTÜ : Orta Doğu Teknik Üniversitesi

OECD : Organisation for Economic Co-Operation and Development

PC : Personal Computer

SBE : Sosyal Bilimler Enstitüsü

SPAM : İstenmeyen Elektronik Posta

SQL : Structured Query Language

TBK : Türk Borçlar Kanunu

TBMM : Türk Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

TCP/IP : Transmission Control Protocol/ Internet Protocol

TDK : Türk Dil Kurumu

TTK : Türk Ticaret Kanunu

TUBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu

URL : Uniform Resource Loader

YÖK : Yükseköğretim Kurumu

WAN : Wide Area Network

WAP : Wireless Application Protocol

Wi-Fi : Wireless Fidelity

WWW : World Wide Web

GİRİŞ

Tarihsel süreç içerisinde insanlık hayatı kolaylaştırıcı teknik ve bilimsel birçok gelişmeye imza atmış ve gelişimini sağlayarak bugünlere ulaşmıştır. Bilgisayarın ve internetin ortaya çıkmasıyla ise bu gelişim hız kazanmış ve her an yeni teknolojilerin ortaya çıkmasına zemin hazırlamıştır. Teknolojinin gelmiş olduğu nokta günlük hayata dair birçok iş ve işlemin bilişim sistemleri ile kolay ve hızlı bir biçimde yapılabilmesini sağlayarak, sosyal hayat, ulaşım, güvenlik, sağlık, eğitim, üretim ve sanayi gibi akla gelebilecek birçok alanda etkin ve yaygın bir biçimde kullanılmasına imkân vermiştir. Tüm bu gelişmelerle birlikte bilişim sistemlerinin anonim bir biçimde hareket etmeye ve dünyada internetin bulunduğu her noktaya erişim sağlamaya imkan veren yapısı art niyetli kişileri de cezbederek bilişim sistemlerinin kullanıldığı birçok alanı tehlikeye sokmuştur. Bilişim alanının ve kullanıldığı tüm mecraların hukuken korunabilmesi için ise birçok devlet ceza kanunlarında bilişim sistemleri aracılığıyla ve bunlar aleyhine işlenen eylemleri suç olarak düzenleyerek, söz konusu eylemleri yaptırıma bağlamıştır. Bu suçların tespitindeki zorlukla beraber sınır aşan yapısı ise devletlerin bu suçlarla mücadelede gerektiğinde ortak bir biçimde hareket etmesini gerektirmiş ve bu konuda başta Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS) olmak üzere uluslararası işbirliğine yönelik adımlar atılmıştır.

Bilişim teknolojilerinin gelişim hızı değerlendirildiğinde, bilişim alanındaki suçlarla mücadeleye yönelik hukuksal çalışmaların teknolojik gelişmelere yetişmesinin oldukça zor olduğu görülmektedir. Bu durumda hukukun teknolojiye ayak uydurabilmesi için ya sık sık bu konuda yeni düzenleme yapılması gerekmekte ya da oldukça geniş kapsamlı düzenlemelere yer verilerek ortaya çıkabilecek tüm eylemlere yönelik genel kaideler oluşturulması gerekmektedir. Bu konuda; kanun yapım sürecinin çetrefilli yapısı sık sık

düzenleme değişikliğine imkan vermediğinden, bu durum; kanun koyucular tarafından söz konusu hukuki korumanın sağlanmasında açık nokta kalmamasını hedefler şekilde, oldukça geniş kapsamlı ve ucu açık düzenlemelerin ortaya çıkarılmasına zemin hazırlamıştır[1]. Bununla birlikte bilişim alanındaki kavramların da tam oturtulamamasıyla beraber, gerek doktrinde gerek yargı bazında birbirine zıt düşüncelerin ortaya çıkması kaçınılmaz olmuş ve bu durum düzenlemelere yönelik birçok tartışma ve eleştiriye sebebiyet vermiştir. Bilişim suçlarının çeşitliliği ve hukuken geniş bir alanı kaplaması dolayısıyla çalışmamızda bu tartışmaların odak noktalarından biri olan, bilişim suçlarından AKSSS'de verilere ve sisteme müdahaleye yönelik düzenlemeyi karşılayan hükümler içeren ve Türk Ceza Kanunu (TCK) m. 244'te düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları ele alınmıştır.

Hazırlanan çalışma iki bölümden oluşmakta olup, ilk kısımda bilişim alanına ilişkin kavramsal çerçeve çizilerek bilişim suçlarının tarihsel sürecine ve suç işleniş şekilleri ile bu suçların işlenmesinde yaygın kullanılan yöntemlere yer verilmiş, ardından bu suçların ulusal ve uluslararası hukuklardaki yansımasına değinilmiş, son olarak ise genel kapsamıyla Türk Ceza Hukuku'nda Bilişim Alanında Suçlar bölümünde düzenlenen bilişim suçları ele alınmıştır. İkinci bölümde ise tezin konusu olan TCK m. 244'te yer alan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları tartışmalı ve eksik bulunan yönleriyle birlikte incelenmiş, benzer bazı suç tipleriyle karşılaştırması yapılmış ve bu konudaki genel kanaatimizin yer aldığı sonuç bölümüyle sonlandırılmıştır.

[1]Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", *Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi*, 49/3 (1994), 165.

BİRİNCİ BÖLÜM

BİLİŞİM ALANINDA KAVRAMSAL ÇERÇEVE

1.1. Genel Olarak

Günümüzde her geçen gün yeni teknolojilerin ortaya çıkmasıyla beraber, günlük hayata dair birçok iş ve işlem bilişim sistemleri ve internet aracılığıyla görülmeye başlanmış ve bilişim sistemleri hayatın vazgeçilmez bir unsuru haline gelmiştir. Bilişim teknolojileri bankacılık ve alışverişten; iletişim, ulaşım, güvenlik, sağlık, eğitim, üretim ve sanayi gibi daha birçok alanda kullanılmaya başlanmış ve günlük yaşamın geneline yayılmıştır. Günümüzde kişisel veriler başta olmak üzere ekonomik veriler ve ticari sırlar gibi birçok önemli bilgi bilişim sistemleri üzerinde işlenmekte ve korunmaktadır. Kişilerin özel haberleşmeleri ve yazışmaları da yine bilişim sistemleri üzerinden gerçekleşmektedir. Günlük hayata ve iş hayatına dair birçok işlemin bilişim sistemleri aracılığıyla görülmesiyle birlikte günümüzde bilişim, her yaş aralığında yaygın şekilde kullanılan bir mecra haline gelmiştir. Tüm bu gelişme ve kullanımda yaygınlaşma ile beraber, bilişim alanı kötü niyetli kişilerce de istismar edilmeye başlanmış ve bu durum, bilişim sistemlerinin kullanıldığı birçok alanı da tehlikeye sokmuştur. Bilişim sistemlerinde yer alan her türlü verinin ele geçirilebilmesinin yanında, günlük hayatın işleyişini sağlayan ve teknolojiyle sağlanan elektrikten ulaşıma kadar daha birçok alanın kesintiye uğramasına yol açabilecek nitelikte saldırıların yapılabilmesi mümkün hale gelmiştir. Yüksek tehlike oluşturacak nitelikteki bu durumun önlenmesi ve bu alanın hukuken korunabilmesi için Türk Ceza Kanunu'nda bilişim suçları düzenlenmiş ve bu suçlar yaptırıma bağlanmıştır.

Bilişim suçlarının oluşturduğu tehlike, bu suçların klasik diğer suç tiplerinden önemli derecede farklılık arz eden nitelikleri ve sınır aşan yapısı, bu suçlarla mücadelede büyük zorluklar yaşanmasına neden olmaktadır. Bilişim suçlarıyla mücadelede yaşanan zorlukların asgari düzeye indirilmesi için gerekli çalışmaların yapılması elzem olup, sürekli gelişen teknolojiye uyum sağlayan bu suçların güncel bir şekilde incelenmesi ve takip edilmesi büyük önem arz etmektedir.

Bilişim suçları incelenirken öncelikle irdelenmesi ve anlaşılması gereken ise bilişim alanına ilişkin temel kavramlardır. Bilişim suçlarının kapsamı belirlenirken hangi fiillerin suç sayılacağı ve bu suçların hangi platformlar üzerinden işlenebileceği gibi konuların belirlenmesi, buna ilişkin bir çerçevenin çizilmesi önem arz etmektedir. Bilişime ilişkin temel kavramların önemi kanunilik ilkesinin uygulanması açısından da karşımıza çıkmaktadır. Suçta kanunilik ilkesi suç sayılan fiillerin kanunda açıkça düzenlenmesini gerektirirken, cezada kanunilik ilkesi ise suç sayılan fiillere uygulanacak yaptırımların kanunda açıkça düzenlenmesini gerektirmektedir[2]. Bu sebeple bilişim ve bilişim sistemleri kavramlarının doğru bir şekilde tanımlanması ve anlaşılması kanunilik ilkesinin de bir gereği haline gelmektedir. Örnek verecek olursak: TCK m. 243'te "Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girmek" suç olarak düzenlenmiştir. TCK m. 243'te yaptırıma bağlanan fiil bilişim sistemleri üzerinden gerçekleşmekte; bilişim sistemleri bu suçun konusunu oluşturmaktadır[3]. Bu sebeple bilişimin ve bilişim sistemlerinin tanımları ve bilişim sistemleri denildiğinde nelerin anlaşılması gerektiği suçun kapsamının belirlenmesi açısından büyük önem arz etmektedir. Teknolojinin sürekli ve hızlı bir biçimde gösterdiği gelişim ve bu gelişimle birlikte ortaya koyduğu yeni sistem ve uygulamalar, bu alandaki teorik bilgilerin düzenli bir şekilde güncellenerek ortaya konmasını gerektirmektedir.

Bu bölümde, yukarıda açıkladığımız üzere, bilişim alanına ilişkin temel kavramlar incelenerek, bilişim suçlarının konusunu oluşturan bilişim sistemleri ele alınacak ve temel bir kavram çerçevesi oluşturularak bilişim suçlarının incelenmesi

[2] Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, (Ankara: Seçkin Yayınları, 2023), 58.
[3] Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Türk Ceza Hukuku Özel hükümler*, (Ankara: Seçkin Yayınları, 2023), 983.

kolaylaştırılacaktır. Daha sonra ise bilişim suçlarının kavramsal ve tarihsel gelişim sürecinden bahsedilecek ve bu suçların işleniş şekli ve işlenmesinde kullanılan yöntemlerle, mukayeseli hukukta yer alan yaklaşımlara ve uluslararası düzeyde bu suçlarla mücadele konusundaki gelişmelere yer verilecektir. Son olarak ise TCK'da bilişim alanında suçlar bölümünde yer alan bilişim suçlarına ilişkin düzenlemeler incelenerek genel hatlarıyla ortaya konulacaktır.

1.2. Bilgi

Bilgi kavramı Türk Dil Kurumu Sözlüğünde "*İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü*", "*Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek*", "*insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü*", "*Duyu organları yoluyla algılama, hayal gücü ve bellek yardımıyla zihnin ilk olarak kavradığı temel düşünceler*" ve "*Verinin anlam kazanmış biçimi*" olmak üzere farklı şekillerde tanımlandığı görülmektedir[4]. Bilgi kavramı başlangıçta felsefenin ilgi alanı içerisinde görülmekteyken bilimsel alanların ortaya çıkışıyla diğer bilim dallarının da tartışma konusu haline gelmiş ve her bilim dalı kendi çalışma alanına göre bilgi tanımını geliştirerek bilgi kavramının anlam genişliğini ortaya koymuştur[5]. Bununla birlikte zaman içerisinde değişen koşullara göre tanımlarda değişikliğe gidilmesi de bilgi kavramının değişken bir kavram olduğunu ortaya koymuştur[6]. Bilgi kavramı disiplinler arası bir kavram olduğundan bütün ve kapsayıcı bir tanım yapılması zordur[7]. Bununla birlikte bilgi kavramının tanımlanmasındaki karmaşanın temel sebeplerinden birisi veri (Data), bilgi (Information) ve bilgi (knowledge) sözcüklerinin çoğunlukla aynı anlamda kullanılmasıdır[8]. "Knowledge" anlamında bilgi "information" anlamında bilgiden sonraki bir aşamayı ifade etmekte olup bilginin yorumlanması ve işlenmesini ifade

[4] TDK sözlük, (E. T. 15.01.2025), https://sozluk.gov.tr/.
[5]Nazan Özenç Uçak, "Bilgi: Çok Yüzlü Bir Kavram", *Türk Kütüphaneciliği Dergisi*, 24/4 (2010): 706.
[6]Uçak, "Bir Kavram", 706.
[7]Nazan Özenç Uçak, "Bilgi Üzerine Kuramsal Bir Yaklaşım", *Bilgi Dünyası Dergisi*, 1/1 (2000): 143-145.
[8] Nazan Özenç Uçak, "Bilgi Üzerine", 146.; Malik Yılmaz, "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi Ve Bilgi Yönetimi", *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49/1 (2009): 98.

etmektedir[9]. Information anlamında bilgi ise kısaca; "*bir durum, kişi, olay vb. hakkındaki gerçekler ya da olgular*[10]"' olarak ifade edilebilir.

1.3. Bilişim

Bilişim terimi ilk kez Steinbuch'un 1957'de yazmış olduğu "İnformatics: Automatic Information Processing" başlıklı makaleyle birlikte ortaya çıkmakla beraber, kavramın yaygınlaşması 1970'lerde OECD'nin bu kavramı yayınlarında kullanılmasıyla olmuştur[11]. 1970'li yıllarda OECD bilişim kavramını kullanırken, bilişim kavramını; bilginin içeriğinin, sunumunun ve bilgi teknolojisinin kullanımıyla ilgili yöntem ve stratejilerin incelenmesi olarak tanımlamıştır[12]. Bilişim sözcüğü kökensel olarak Fransızca "İnformatique" sözcüğünden gelmekle birlikte, Türkçede ilk kullanımı bu sözcüğün Türkçeye çevrilmesiyle elde edilen ve bilgi vermek anlamını taşıyan enformasyon kelimesi olmuş[13], ilerleyen zamanda ise yerini Aydın Köksal'ın önerisiyle ortaya atılan bilişim sözcüğüne terk etmiştir[14]. Bilişim kelimesinin bilgi ve matematik kavramlarının birleşiminden oluştuğu ifade edilmekle birlikte, bir diğer oluşum şeklinin ise "İnformation" ve "Automatik" yani bilgi ve otomatik kelimelerinin birleşmesi olduğu ifade edilmektedir[15].

Bilgisayar ve bilişim kelimelerinin çoğu zaman iç içe geçtiği ve bu kavramların bir diğeri yerine kullanıldığı görülse de aslında bilgisayar bilişime göre daha alt bir kavramı ifade etmekte, bilişim sürecinin içinde yer alan bir araç konumunda kalmaktadır[16].

---

[9] Nazan Özenç Uçak, "Bilgi Üzerine", 147.
[10] Cambridge Dictionary, (E. T. 28.02.2025), https://dictionary.cambridge.org/.
[11] Semanur Öztemiz, "Sosyal Bilişim Üzerine Kavramsal Bir Değerlendirme", *Bilişim Teknolojileri Dergisi*, 11/ 4 (2018), 311.; P. Fichman, H. Rosenbaum, *Social informatics: Past, present and future.*, (Newcastle, UK: Cambridge Scholars Publishing, 2014), 7.
[12]P. Fichman, H. Rosenbaum, *Social informatics.*, 7.
[13] Murat Volkan Dülger, *Bilişim Suçları Ve İnternet İletişim Hukuku*, (Ankara: Seçkin Yayınları, 2023), 74.; Mesih Gözüşirin, "5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi", (Yüksek Lisans Tezi, Kara Harp Okulu, 2011), 3.; Ali Karagülmez, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, (Ankara: Seçkin Yayıncılık, 2014), 50.; Ahmet Caner Yenidünya ve Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, (İstanbul: Legal Yayıncılık, 2003), 27.
[14] Hayati Pallı, "Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları", (Yüksek Lisans Tezi, Erciyes Üniversitesi,2008), 34.
[15] Metin Turan, *Bilişim Hukuku*, (Ankara: Seçkin Yayınları, 2023), 48.
[16]Burak Cesur Aköz, "Türk Ceza Kanunu Kapsamında Bilişim Suç Ve Cezaları İle Örnek Yargısal Kararların Analizi Ve Mevzuat Önerileri", (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, 2018), 5.

TDK sözlüğünde bilişim; "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun biçimde işlenmesi bilimi*." olarak tanımlanmaktadır[17]. TDK'nın bu tanımından hareketle, bilişim kavramının bilginin elektronik makineler aracılığıyla işlenmesini konu edinen bir bilim dalı olduğu ifade edilebilir. Nitekim bilişimin temel görevleri bir bilim dalı olarak temel aksiyomatik matematiksel kuramlar üreterek, diğer tüm uzmanlık dallarının nesne ve süreçlerini gözlemleyip bunları soyut matematiksel yapılara dönüştürmek ve bunların işlenebileceği sistemleri tasarlamaktır[18].

Doktrinde ise bilişim kavramı özetle; verilerin sanal ortamda üretimi, kaydı, iletimi, saklanması, paylaşımı gibi fiilleri konu edinen bir bilim dalı[19]; ekonomik ve toplumsal iletişimde kullanılan bilginin elektronik araçlarla işlenip aktarılması[20]; bilgisayarlardan yararlanılarak verinin saklanması, iletilmesi ve işlenmesini konu alan akademik ve mesleki disiplin gibi birçok farklı şekilde ifade edilmektedir[21]. Doktrinde bilişim kavramına ilişkin yapılan tanımlamaların birçoğunun temelinde kavramın ortak noktasının sistemler aracılığıyla veri işleme ve veri aktarımı yapılması olduğu ifade edilmektedir[22].

Yer verdiğimiz tanımlardan da görüldüğü üzere bilişim kavramı tanımlanırken oldukça geniş kapsamlı ifadeler kullanılmakta ve teknik anlamda bilgisayar ifadesine indirgenmemektedir. Bu konuda doktrinde; bilgisayarın verileri depo etme, saklama yeniden değerlendirme gibi faaliyetlerde bulunurken, bilişimin bu faaliyetlerin yanında veri iletişimini de gerçekleştirmesi dolayısıyla bilişimin bilgisayara göre daha üst bir kavram ifade ettiği dile getirilmiştir[23]. Kaldı ki -tanımından da anlaşılacağı üzere- bilişim bir bilim dalıdır. Bilgisayar ise bir araçtır. Bu konuda verilen bir örneklemeyle bilişimin bilgisayarla ilgisinin, astronominin teleskopla ilgilisiyle aynı düzeyde olduğu

[17] TDK sözlük, (E. T. 15.01.2025), https://sozluk.gov.tr/.; Aydın Köksal, *Bilişim Terimleri Sözlüğü*, (Ankara: Türk Dil Kurumu Yayınları, 1981), 28.
[18] Pallı, "Hukukta Bilişim Suçları", 34.
[19] Turan, *Bilişim Hukuku*, 50.
[20] Ahmet Gül, *Doğrudan - Dolaylı Bilişim Suçları*, (Ankara: Seçkin Yayınları, 2021), 35.; Akbulut, Bilişim Alanında Suçlar, (Ankara: Adalet Yayınevi, 2017), 13.; Doğan Soyaslan, *Ceza Hukuku Özel Hükümler*, (Ankara: Yetkin Yayınları, 2016), 633.
[21] Pallı, "Hukukta Bilişim Suçları", 34.
[22] Dülger, *İnternet İletişim Hukuku,* 71.
[23] Uğur Özüdoğru, "Siber Suçlar ve Mücadele Yöntemleri Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri", (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, 2011), 6.; Yenidünya ve Değirmenci, *Mukayeseli Hukukta,* 31.

ifade edilmektedir[24]. Bu anlamda bilgisayarlar birer bilişim sistemi olmakla birlikte bilişim kavramı yalnızca bilgisayarları ifade etmemekte; bilişim sistemi de yalnızca bilgisayarlarla sınırlı olmayıp, bunun yanında cep telefonları ve elektronik güvenlik sistemleri gibi birçok elektronik aygıt da yine bilişim sistemi olarak kabul görmektedir[25]. Bunun sebebi ise teknolojinin gelişmesiyle birlikte sürekli gelişen bilişim alanının giderek bu alanda bir araç konumunda olan klasik bilgisayar sistemlerinin ötesine geçen farklı bilişim sistemleri dizayn etmesi ve bu yeni üretilen sistemlerin de birer bilişim sistemi olduğunun kabulüdür.

1.4. Bilişim Teknolojileri ve Bilişim Sistemleri

Bilişim teknolojileri TDK sözlüğüne göre; "*Bilişimde kullanılan bütün araç ve gereçlerin oluşturduğu sistemler."* olarak tanımlanmıştır[26]. Doktrinde yapılan tanıma göre ise bilişim sistemleri; "*Verilere ilişkin bir takım saklama, nakletme, çoğaltma ve düzenleme gibi fonksiyonları otomatik gerçekleştiren sistemler*" olarak tanımlanmıştır[27].

5237 sayılı TCK'nın tasarı metninde yer alan ve Adalet Komisyonu'nca m. 243 olarak kabul edilen m. 346.'nın gerekçesinde ise; *"Bilişim alanından maksadın verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler olduğu ve bu uzun tanımlamanın yerine kısaca bilişim sistemi ibaresinin kullanılacağı…"* ifade edilmiştir[28]. Doktrinde madde gerekçesinin bu şekilde açıklanmış olmasının sebebinin gelişen teknoloji dolayısıyla birden fazla sistem aracılığıyla bu suçların işlenebileceğini ifade etmek olduğu belirtilmiştir[29].

[24] Pallı, "Hukukta Bilişim Suçları", 34.
[25] Dülger, *İnternet İletişim Hukuku,* 71.
[26] TDK sözlük (E. T. 15.01.2025), https://sozluk.gov.tr/
[27] Özbek, Doğan ve Bacaksız, *Özel hükümler*, 991.
[28] "Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu (1/593)", (E. T. 15.01.2025), https://cdn.tbmm.gov.tr/KKBSPublicFile/D22/Y1/T1/DosyaKomisyonRaporunuVerdi/08f04456-d914-428b-8ee5-49694952fd88.htm
[29] Uğur İhtiyaroğlu, "Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi", *Hacettepe Hukuk Fakültesi Dergisi* 10/2 (2020): 408.

AKSSS'nin yaptığı tanıma göre bilişim sistemi; "*Bir veya birçok unsuru, bir programın işleyişi aracılığıyla verilerin otomatik olarak işleme tabi tutulmasını sağlayan, birbirine bağlanmış veya benzeşen tek veya toplu tertibat*" olarak ifade edilmiştir[30].

Yargıtay Ceza Genel Kurulu'nun 2009 tarihli bir kararında bilişim sistemi "*Verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağı veren manyetik sistemler."* olarak tanımlanmış, bilişim alanı ise yine aynı kararda "*Bilgileri depo ettikten sonra bunları otomatik olarak işleme tabi tutan sistemlerden oluşan alanlar."* olarak ifade edilmiştir[31].

Doktrinde tanımlarda bilişim sisteminin "manyetik sistem" olarak tanımlanmasıyla manyetik olmayan bir sistemin bilişim sistemi olarak düşünülemeyecek hale getirildiği; "verileri toplayıp yerleştirme" eyleminde ise, eylemin kim tarafından gerçekleştirildiği ve verilerin nereye yerleştirileceği hususunda bir ifadeye yer verilmediği ifade edilerek bu tanımlar yetersiz görülmüş ve eleştirilmiştir[32]. Bu konuda başka bir eleştiride de tanımın bilişim alanını ifade etmekte yetersiz olduğu, "manyetik sistem" ibaresi ile bilgisayarlar içerisinden yalnızca manyetik nitelikli bilgisayarların anlaşıldığı, bu sebeple yetersiz ve hatalı bir tanımlama olduğu ifade edilmiştir[33].

Bilişim sistemi tabirinden ne anlaşılması gerektiği konusunda önceki dönemlerde farklı görüşler mevcut iken, gelinen son durumda bu konuda bir takım değişiklikler olduğu görülmektedir. Bilişim suçlarının ilk ortaya çıktığı dönemlerde teknolojinin gelişmişlik seviyesine bağlı olarak ve bu suçların genellikle bilgisayarlar üzerinden gerçekleştirilmesi dikkate alınarak bilişim sistemi kavramının temelde bilgisayar tabanlı olarak ifade edildiği görülmektedir. Buna göre; eğer ortada bir bilgisayar olmadan çalışamayan bir sistem varsa, bu durumda bu sistemin bilişim sistemi olduğunun kabulü gerekeceği ölçütlerden biri olarak kabul edilirken; ikinci bir ölçüt, bilgiyi otomatik işleyebilen sistemler olması; üçüncü ölçüt ise sistemin genel amaçlı programlanabilmesi

---

[30] Cengiz Apaydın, *Bilişim Suçları ve Bilişim Ceza Hukuku*, (İstanbul: Acar Matbaacılık, 2017), 153.; "Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001", (E. T. 15.01.2025) https://www.coe.int/en/web/cybercrime/the-budapest-convention

[31] Yargıtay Ceza Genel Kurulu, 17.11.2009, E. 2009/11-193 K. 2009/ 268, https://www.kazanci.com.tr/, E. T. 15.01.2025.

[32] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 992.

[33] Yılmaz Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi", İçinde *Yeni Türk Ceza Kanunu Sempozyumu*, (İstanbul: Türk Ceza Hukuku Derneği Yayını, 2005), 112.

olarak değerlendirilmiştir[34]. Bu kapsamda ATM[35] ve bilgisayarlar bilişim sistemi olarak kabul edilmişken; cep telefonları bilişim sistemi kapsamında sayılmamışlardır[36]. İlerleyen dönemlerde ise bilişim sistemi ile bilgisayar kavramları arasındaki tanım farkı giderek açılmış ve bilgisayar temel ölçüt olarak görülmemeye başlanmıştır. Bu konuda Yargıtay'ın 2021 tarihli bir kararında bilişim sisteminin kavramsal olarak yalnızca bilgisayar yahut internetle sınırlı tutulmaması gerektiğinin altı çizilmiştir. Buna göre bilişim sistemi tabiri her geçen gün gittikçe hız kazanan teknolojik gelişmelere ayak uyduracak şekilde tüm bilişim teknolojilerini kapsamalıdır[37].

Teknolojinin gelişmesiyle birlikte günlük hayatta kullandığımız birçok elektronik eşyanın işletim sistemlerine sahip versiyonları çıkarılmış ve bu elektronik eşyalar genel olarak "akıllı" tabiriyle nitelendirilmeye başlanmıştır. Örneğin; cep telefonlarında android, IOS gibi işletim sistemlerinin kullanılmaya başlanması ve böylece bunların da ufak birer bilgisayar formatına bürünmesi, günümüzde cep telefonlarının da bilişim sistemi olarak kabulünü mümkün hale getirmiştir. Doktrinde de bilgisayar dışındaki diğer bazı aygıtların bilişim sistemi olarak değerlendirilebilecek özelliklerinin olduğu, cep telefonları, WAP uyumlu elektronik ev aletleri ve benzeri elektronik araçlar üzerinde veya bunları bağlayan ağlar üzerinde bilişim suçlarının işlenebileceği vurgusu

---

[34] Ş. Cankat Taşkın, "Bilişim Hukuku Uluslararası Uyuşmazlıklar", *TBB Dergisi*, 85 (2009): http://tbbdergisi.barobirlik.org.tr/m2009-85-571, 334.

[35]Yargıtay ATM'leri bilişim sistemi olarak kabul etmiş, gerekçesini şu şekilde açıklamıştır: *"...Kısaca ATM olarak da adlandırılan Automated Teller Machine sisteminin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura gereksinim vardır, bunlardan birincisi kart diğeri ise kullanıcı şifresidir. Bu iki araca sahip olmadan, bir bilgi işlem biriminin parçası olan ve ana sisteme bağlı bulunan ATM makinelerini kullanma olanağı yoktur. Belirtilen karta ve şifreye sahip olan kişi, kartı makineye takıp şifreyi de yazdıktan sonra işlem sürecini başlatabilir. Ancak, kartı elinde bulunduran kişinin makine vasıtasıyla sisteme verdiği komutların yerine getirilebilmesi için ana kumanda merkezinin de bu komutları onaylaması gerekmektedir. Örneğin nakit para çekilmek istendiğinde hesapta para yoksa veya günlük çekme limiti dolmuş yada herhangi bir nedenle hesap ana merkez tarafından kullanıma kapatılmışsa işlem, komut onaylanmayacağından yapılamaz. Bu olgu da gösteriyor ki ATM makineleri bir bilgi işlem sisteminin ünitesidir. Yine, sistemi harekete geçirmede kullanılan kartların geleneksel hırsızlık suçları bakımından "sair alet" olarak kabul edilmesi de olanaklı değildir..."* Yargıtay Ceza Genel Kurulu, 11.04.2000, E. 2000/6-62 K. 2000/72, , https://www.kazanci.com.tr/, E. T. 15.01.2025.

[36] Taşkın, "Uluslararası Uyuşmazlıklar", 334.

[37]Bilişim sistemleri kavramından ne anlaşılması gerektiğini Yargıtay bir kararında şu şekilde açıklamaktadır: *"...Bilişim sistemi denince akla önce bilgisayar ve internet gelmekte ise de, bilişim sisteminin kapsamı çok geniş olup, bilginin toplanmasında, işlenmesinde, depolanmasında, ağlar aracılığıyla bir yerden bir yere iletilip kullanıcıların hizmetine sunulmasında kullanılan iletişim ve bilgisayarlar dâhil bütün teknolojileri kapsar. O halde bilişim sistemi öncelikle bilişim teknolojisini kapsamalıdır. Peki bilişim teknolojisi nedir? Bilişim teknolojisi, iletişim ve bilgisayar sistemleriyle bağlanabilen bilgi hizmetlerinin tamamı için kullanılan bir kavramdır. Yani bu kavram sadece bilgisayar donanım ve yazılımlarıyla veya internet ile sınırlı tutulmamalıdır..."* Yargıtay Ceza Genel Kurulu, 2.3.2021, E. 2018/23-51, K. 2021/68, https://www.kazanci.com.tr/, E. T. 15.01.2025.

yapılmıştır[38]. Bununla birlikte bu tarz aletlerin her zaman bilişim sistemi olarak kabul edilmemesi gerektiği, yalnızca belirli işlemleri otomatik bir biçimde gerçekleştirebilen, tek amaçlı elektronik veyahut manyetik cihazların bilişim sistemi olarak değerlendirilmemesi gerektiği düşüncesi de mevcuttur[39]. Yargıtay 2015 tarihli bir kararında cep telefonlarında mobil işletim sistemleri bulunması ve cep telefonlarının program yüklenebilir hale gelmesi dolayısıyla, bunlar açısından bilişim sistemine girme ve orada kalma suçunun oluşup oluşmadığının somut olayda tespit edilmesi gerektiğine ve bu inceleme yapılmadan salt cep telefonlarının bilişim suçu oluşturmayacağından bahisle verilen kararın hatalı olduğuna hükmetmiştir[40].

Yargıtay'ın bu konudaki kararlarından da anlaşılacağı üzere, zaman içerisinde teknoloji geliştikçe bilişim sistemleri çeşitlenmekte ve dolayısıyla daha önce var olmayan yeni bilişim sistemleri ortaya çıkmaktadır. Bu durumun doğal bir sonucu olarak da bilişim alanında yapılan tanımlamaların doğru ve geleceği kapsayıcı şekilde yapılması önem arz etmektedir. Günümüze kadar yapılan tanımlamaların birçoğu aşağı yukarı aynı ifadeleri kapsamakta ve bu çerçeveyi geniş tutmaya çalışmaktadır. Bu durum da alanın gelişim hızı düşünüldüğünde son derece yerindedir. Ancak günümüz koşulları her ne kadar yapılan bu tanımlamaları kabule elverişli olsa da, ilerleyen yılların getireceği teknik gelişmeler göz önüne alındığında, bilişim sektörü kadar, bu sektöre ilişkin tanımların dahi değişme ihtimalinin bulunduğu açıktır.

1.4.1. Bilgisayar

Tarih boyunca insanlık, sayısal ve rakamsal işlemleri kolaylaştırmak adına farklı icatlar geliştirilerek bu işlemlere ayıracakları vakitten tasarruf sağlamak istemiştir. Bu amaçla milattan önce 3000 yıllarında Çin'de icat edilen ve bilgisayarların atası olarak kabul edilen abaküs etkili bir araç olarak kabul edilmiş ve binlerce yıl kullanılmıştır. 1944 yılında otomatik bilgisayarların atası sayılan ve hesaplayıcı işlevi gerçekleştiren Mark1

[38] Sacit Yılmaz, "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", *TBB Dergisi*, 92 (2011), 63.; Caner Yenidünya, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu", *Legal Fikri ve Sınaî Haklar Dergisi*, 4 (2005):https://legal.com.tr/Book/X52MjOnHHkOTJlqh-kLcOA/891d454613394b65b41078c6f61b0559?s=&pn=69 ,1030.

[39] Nebahat Kayaer, "Türk Hukukunda Bilişim Sistemine Girme Suçu (TCK. m. 243)", *Ceza Hukuku Dergisi*, 14/39 (2019), 94.

[40] Yargıtay 8. Ceza Dairesi, 18.03.2015, E. 2014/30037, K. 2015/14023, https://kararara ma.yargitay.gov.tr/, E.T. 15.01.2025.

icat edilmiş, 1945 yılında ise Mauchly ve Eekert tarafından ilk sayısal elektronik bilgisayar olan ENİAC üretilmiş; bu tarihten itibaren üretilen bilgisayarlar ise 5 kuşağa ayrılarak sınıflandırılmaya başlanmıştır[41]. 1. Kuşakta 1946-1954 yılları arasında üretilen vakum tüplü bilgisayarlar; 2. Kuşakta 1959-1964 yılları arasında kullanılan transistörlü bilgisayarlar; 3. Kuşakta 1964-1970 yılları arasında üretilen entegre devreli bilgisayarlar; 4. Kuşakta 1970 ve sonrasında üretilen, günümüzde de halen daha kullanılan, önceki dönemlere göre çok daha kullanışlı ve taşınabilir nitelikte bulunan mikro işlemcili bilgisayarlar; 5. Kuşakta ise 1990 ve sonrasında üretilen ve halen daha geliştirilmeye çalışılan yapay zekalı bilgisayarlar yer almaktadır[42].

Bilgisayar denildiğinde ilk akla gelen klasik anlamda günlük hayatta kullandığımız masaüstü veya dizüstü bilgisayarlar olsa da bu kavramın aslında bunlardan çok daha fazlasını ifade ettiği söylenebilir. TDK'nın tanımına göre bilgisayar; "*Belleğine yüklenmiş program uyarınca aritmetik ve mantık işlemleri yapabilen, sonuca göre karar verip programdaki akışı değiştirebilen, çevresiyle etkileşimde bulunabilen, girdi ve sonuç verilerini belleğinde tutabilen aygıt; elektronik beyin*." olarak tanımlanmaktadır[43]. Bilgisayar genel olarak verileri (Ham bilgileri) işleyerek bilgiye dönüştüren elektromekanik cihazlar olarak tanımlanmaktadır[44].

AKSSS'nin tanımlamaları içeren maddesi olan m. 1.'de "Computer System" olarak ifade edilen bilgisayar sistemi "*Bir program çerçevesinde, otomatik veri işleme faaliyeti gerçekleştiren bir yahut birbirine bağlı veya birbiriyle ilişkili birden fazla cihaz ya da cihaz grupları.*" olarak tanımlanmıştır[45].

Bilgisayarın tanımlamasının çoğunlukla iki şekilde yapıldığı görülmektedir. Birinci şekilde yapılan tanımlama daha çok bilişsel özellikleri dikkate alırken, ikinci tanım bilgisayarın soyut - somut tüm özellikleri dikkate alınarak yapılmaktadır[46].

[41] Bu konuda detaylı bilgi için bkz: Hafize Keser, "Bilgisayarın Evrimi", *Ankara University Journal of Faculty of Educational Sciences (JFES)*, 24/2 (1991), 411-415.
[42] Keser, "Bilgisayarın Evrimi", 414 vd.
[43] TDK sözlük, (E. T. 15.01.2025), https://sozluk.gov.tr/
[44] Cem S. Sütçü, "Bilgisayar ve Bilgisayar Ağları", *Marmara İletişim Dergisi*, 5/5 (1994), 145.
[45] "Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001"
[46] Dülger, *İnternet İletişim Hukuku,* 64.

İlk tanıma göre bilgisayar; her tür problem üzerinde çalışabilen ve genel amaçlı kullanılabilen bir cihazdır[47]. Veriyi işleyebilme ve bir anlam dâhilinde açıkça ifade edilen tüm problemleri çözebilme kabiliyetine sahip olması bir bilgisayarda aranan temel özelliktir[48]. İkinci tanıma göre ise; dış ortamdan elde ettiği verileri üzerine yüklenen programlar vasıtasıyla muhafaza etme, iletme, mevcut veriden yeni veri üretme ve başka yerdeki verilere ulaşma gibi amaçlarla kullanılan bir makinedir[49]. Bilgisayarın en önemli özelliklerinden biri ise girilen verileri değerlendirerek ve bunları bir sonuca bağlayarak istenilen çıktının elde edilebilmesidir.

Klasik bir bilgisayar sistemi, çalışmasını sağlayan birtakım unsurlardan oluşur. Bu unsurlar, bilgisayarın fiziksel bir takım birimlerden oluşan "*donanım*" ve veri işleme özelliğini sağlayan "*yazılım*" kısımlarıdır. Bilgisayarın donanım kısmı, merkezi işlem birimi (CPU), ana bellek, depolama, girdi ve çıktı birimlerinden oluşur[50]. Yazılım kısmı ise bilgisayarın kendi çalışmasını yürüten sistem yazılımları ve kullanıcı için hazırlanmış çeşitli programlardan oluşan uygulama yazılımları olmak üzere iki çeşit olarak karşımıza çıkar[51]. Tüm bu yazılım ve donanım bir bütün halinde bilgisayar sistemini oluşturur. Donanımı bilgisayarın vücudu olarak düşünürsek, yazılım bilgisayarın beynini ifade eder.

Bilgisayarın verileri bilgiye dönüştürme faaliyetine kısaca bilgi işlem denir[52]. Bilgi işlem faaliyeti öncelikle verilerin kaydı ile başlar[53]. Veri kaydından sonra sınıflama, sıralama, hesaplama, özetleme gibi bir takım düzenleme faaliyetleri yürütülür[54]. Çıktı faaliyetleri ise depolama, istendiği zaman tekrar aranan bilgiye kolayca ulaşabilme olarak tanımlayabileceğimiz çağırma işlemi, çoğaltma ve iletişim faaliyetleridir[55].

Bilgisayarların en önemli özelliklerinden biri de veri iletişimini sağlamalarıdır. Ancak bu veri iletişiminin sağlanabilmesi için bilgisayarların aynı dili konuşabiliyor olmaları

[47]Dülger, *İnternet İletişim Hukuku,* 64-66.
[48]Berrin Bozdoğan Akbulut, "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 8/1-2 (2000), 546.
[49]Dülger, *İnternet İletişim Hukuku,* 61.; Yenidünya ve Değirmenci, *Mukayeseli Hukukta,*19.
[50]Davut Özkul, "Bilişim Sistemi Kavramı Ve Bilişim Sistemlerinin Denetimi", *Sayıştay Dergisi*, 13/44-45 (2002), 14.
[51]Özkul, "Bilişim Sistemlerinin Denetimi", 16.
[52] Sütçü, "Bilgisayar Ağları", 146.
[53] Sütçü, "Bilgisayar Ağları", 146-148.
[54] Sütçü, "Bilgisayar Ağları", 146-148.
[55] Sütçü, "Bilgisayar Ağları", 148.

gerekmektedir. Bu veri iletişimi ise "0" ve "1" biçiminde kodlanan bir verinin bilgisayarlar arasında alışverişi ile sağlanmaktadır[56]. İkilik sistemi olarak ifade edilen bu kodlama biçiminde elektrik işaretinin polarizasyon seviyelerini ifade eden ve yüksek seviye işareti olan "1" ile alçak seviye işareti olan "0"'lar birbiri peşine dizilerek önceden belirlenen kodlara göre karakter ve sayıları oluşturur[57]. İşte, tüm bu sayısal kodları bir araya getiren, bunlar yoluyla veri oluşturup iletişim kurabilen, bilişim teknolojilerinin en bilindik ve en yaygın kullanılanı olarak karşımıza çıkan cihaz, bilgisayarlardır.

Bilgisayarlar, bilişim suçlarının işlenmesinde oldukça önemli bir araç konumunda olsa da, ortada bir bilgisayar olmadan da bilişim suçlarının işlenebilmesi mümkündür. Bunun sebebi ise günümüz şartlarında tüm bu belirttiğimiz özelliklerin yalnızca bilgisayarlarda değil, diğer akıllı cihazlarda da görülebiliyor olmasıdır.

1.4.2. Ağ ve İnternet

Ağların ağı anlamına gelen internet ilk kez ABD'de 1962'de ARPANET (Advanced Research Projects Agency Network) ile Massachusetts Institute of Tecnhnology'nin galaktik ağ kavramıyla bir psikolog olan Joseph Carl Rebnett Licklider[58] tarafından ortaya atılmış ve ilk internet bağlantısı 1969'da dört merkez arasında ARPANET tarafından gerçekleştirilmiştir[59]. 1983'de iletişim kontrol protokolü yani günümüzde varlığını sürdüren ve temel ana internet ağı halkası olan TCP/IP yürürlüğe girmiş, ilk başta askeri amaçlarla geliştirilen internet 1995'ten itibaren askeriyeden ayırılıp tamamen özelleştirilmiştir[60]. Diğer iletişim ortamlarına göre hızlı gelişim göstermesi ve yeniliklere uyum sağlayan bir yapıda olması sebebiyle en büyük sosyal olgulardan birine dönüşerek günlük iletişimde önemli bir konuma gelmiştir[61].

---

[56] Fatih Ertam, "Bilgisayar Ağları Ve İnternet Üzerinden Başka Bir Bilgisayarın Kontrolü" (Yüksek Lisans Tezi, Fırat Üniversitesi, 2005), 4.
[57] Cüneyt Bergel, "Bilgisayar Ağları ve Güvenlik", *SAU Fen Bilimleri Enstitüsü Dergisi*, 8/1 (2004), 5.
[58] Oğuz Turhan, "Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar)", (Planlama Uzmanlığı Tezi, TC. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, 2006), 7.
[59] Bkz: Hamza Çakır ve Hakan Topçu, "Bir İletişim Dili Olarak İnternet", E*rciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 19 (2005), 75.
[60] Bkz: Çakır ve Topçu, "Bir İletişim Dili", 75.; Oğuz Turhan, "Bilgisayar Ağları ile", 7.
[61] Şerafettin Ekici, "Bir İletişim Ortamı Olarak İnternet ve Türkiye'de İnternetin Regülasyonu", (Yüksek Lisans Tezi, Marmara Üniversitesi, 2009), 29.

Türkiye'de ise ilk internet bağlantısı 90'ların başında TUBİTAK ile ODTÜ'nün işbirliğiyle gerçekleştirilmiş ve 1993'te TR-NET projesi ortaya atılmıştır[62]. Bu projeyle internetin bireysel kullanıcılar ile özel şirketler tarafından da kullanımı sağlanarak 1995 yılının başlarında 3000'den fazla kullanıcıya ulaşılmış, ilerleyen yıllarda ise kullanıcı sayısı katlanarak artarak ülke genelinde internet kullanımı yaygınlaşmaya başlamıştır[63].

Ağ *(network)* temelde veri paylaşımını sağlayan ve birden çok cihazı birbirine bağlayan teknolojiye verilen addır[64]. En az iki cihaz olmakla birlikte, dünyanın herhangi bir yerinde bulunan sayısız cihazı birbirine bağlayabilen bu ağ bağlantısı, kablo ile veyahut mikro dalgalar veya uydular aracılığıyla sağlanabilir[65]. İnternet ise bu paylaşımı sağlayan ve birbirine bağlı birden çok ağdan oluşmaktadır[66]. 1985'den itibaren küresel olarak kullanılmaya başlayan ve İnterconnected Networks kavramının kısaltılarak oluşturulan network (internet) kavramsal olarak "*kendi aralarında bağlantılı ağlar*" anlamına gelmektedir[67].İnternet kavramını günlük kullanımda "*World Wide Web (www)"* yani Türkçeye çevirisiyle *"Dünya Çapında Ağ"* olarak da ifade edilse de[68]; aslında aynı kavramı karşılamamaktadır[69]. Birçok internet hizmetini bünyesinde birleştiren bir araç olan World Wide Web; yazı, resim, ses, video, animasyon gibi farklı nitelikteki verilere ulaşım sağlayan bir çoklu hiper ortam sistemidir[70]. İnternet ise ağın fiziksel yönünü ifade eder[71].TDK sözlüğünde ise internet kavramı "*Genel Ağ*" olarak ifade edilmektedir[72]. Birden çok şekilde dile getirilebilen internet günümüzde dünyayı birbirine bağlayan ve küresel çerçevede etkileşime imkân sağlayan devasa bir iletişim vasıtası olarak karşımıza çıkmaktadır.

---

[62] Peter Wolcott, "The Diffusion Of The Internet In The Republic Of Turkey", *University of Nebraska*, (1999), 19.
[63] Peter Wolcott and Kursat Çağıltay, "Telecommunications, Liberalization, and the Growth of The Internet in Turkey", *Information Society*, 17/2 (1999), 137.
[64] Bkz: Özkul, "Bilişim Sistemlerinin Denetimi", 17.
[65] Bkz: Turhan, "Bilgisayar Ağları ile", 4.
[66] Ertam, "Bilgisayarın Kontrolü", 9.
[67] Eymen Görgülü, "İnternet'in Öyküsü: Geçmişten Günümüze", *Bilişim Kültürü Dergisi*, 2 (2021), 92, https://www.bilisimdergisi.org.tr/bilisim-dergisi-temmuz-2021#bilisim-dergisi-temmuz-2021/6/.
[68]Görgülü, "İnternet'in Öyküsü", 92.
[69] Turhan, "Bilgisayar Ağları ile", 10.
[70] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, "Dijitalleşen Dünyada Bilişim suçları ve Mücadele Yöntemleri", *Bilgi Teknolojileri ve İletişim Kurumu,* (2022), 9. https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/dijitallesen-dunyada-bilisim-suclari-ve-mucadele-yontemleri-6218e2417eaea.pdf
[71] Turhan, "Bilgisayar Ağları ile", 10.
[72] TDK sözlük, (E. T. 15.01.2025), https://sozluk.gov.tr/.

En yaygın bilgisayar ağları yerel bilgisayar ağları (LAN) (Local Area Network), geniş alan bilgisayar ağları (WAN) (Wide Area Network) ve şehirsel bilgisayar ağları (MAN) (Metropolian Area Network) olmak üzere başlıca üç çeşittir[73]. İnternet ise tüm bunların üzerinde küresel bir ağlar bütünü olarak karşımıza çıkmaktadır[74]. Bir sınırlayıcı ve yöneticiye sahip olmayan[75] internet dünyası kullanıcı, telekomünikasyon idareleri, internet servis sağlayıcıları (ISS) gibi önemli süjelerin bir araya gelmesiyle oluşur[76].

Bilgisayarların birbiri ile iletişimini sağlayan internet, belli kurallara tabi şekilde bu iletişimi yürütür ve bu kurallara ağ protokolleri adı verilir[77]. Ağ protokolleri aslında cihazlar arası iletişimi sağlamak için kullanılan iletişim dilini ifade eder[78]. Protokol denmesinin sebebi ise bilgisayar dili ifadesinin zaten önceden beri kullanılıyor olmasından kaynaklanmaktadır[79]. İnternetin temel ağ protokolü her katmanı ayrı işi gerçekleştiren, temeldeki iki ana katmanıyla adlandırılan ve temel iki katmanla birlikte altındaki dört ayrı katmandan oluşan TCP/IP protokolüdür[80]. İletim kontrol protokolü anlamına gelen Transport Control Protokol (TCP) mesajların doğru yere ulaştırılmasından; internet protokolü anlamına gelen "IP" ise adresleme sisteminden sorumludur[81]. Ağ protokolleri dosya aktarımı, URL'leri IP adreslerine çevirme, e-posta gönderme, uzaktan bir sisteme erişme gibi birçok görevin yerine getirilmesini sağlarlar[82]. Kendi içinde görev dağılımı gerçekleştirilen tüm bu protokoller internetin kurallarını oluşturur ve bu protokoller aracılığıyla iletişim sağlanarak veri transferi yapılması mümkün hale gelir.

[73] Turhan, "Bilgisayar Ağları ile", 5.
[74] Turhan, "Bilgisayar Ağları ile", 6.
[75] Mert Çakıcı, "Türk Ceza Kanunu M. 243 ve M. 244'te Düzenlenen Bilişim Suçları", *Ceza Hukuku Dergisi*, 9/24 (2014), 310.
[76] Bkz: Çetin Gümüş, "Bilişim Suçlarıyla Mücadelede Polisin Eğitimi", (Doktora Tezi, Fırat Üniversitesi, 2008), 25.
[77] Aysel Aksu, "Ağ Protokolleri", (E. T. 15.01.2025), https://sudo.ubuntu-tr.net/ag-protokolleri.
[78] Hamza Şamlıoğlu, "Ağ İletişim Protokolleri ve Portlar", (E. T. 15.01.2025), https://www.priviasecurity.com/ag-iletisim-protokolleri-ve-portlar/.
[79] Şamlıoğlu, "Portlar".
[80] Aksu, "Ağ Protokolleri".
[81] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı , "Dijitalleşen Dünyada", 9.
[82] Şamlıoğlu, "Portlar".

IP adresleri internete bağlanacak cihazların birbirlerini tanıma amacına hizmet eden ve temel olarak veri transferini sağlayan[83]; Tüketici IP adresleri ile Genel IP adresleri gibi farklı kategorilere ayrılan ve her IP adresi dörtlü sayı grupları ile birbirinden benzersiz şekilde oluşturularak elde edilen kimlik numaralarıdır[84]. IP adresleri veri alışverişini sağlamakla birlikte siber güvenlik ve pazarlama gibi konularda da kullanılmaktadır[85]. Özellikle siber suçlar açısından IP adreslerinin büyük önem arz ettiği görülmektedir. Siber suç failleri sosyal mühendislik, çevrimiçi ortamlarda takip, konum izleme, ağ saldırısı ve bunun gibi birçok teknik kullanarak IP adreslerine ulaşmakta, bu şekilde kullanıcıları hedef alabilmekte ve sistemleri ele geçirebilmektedirler[86]. Bu sebeple IP adreslerinin korunması güvenlik açısından oldukça önemlidir.

Bilgisayar ağlarının kurulması teknolojinin gelişim süreci açısından önem arz etmekle birlikte, teknolojik gelişmeleri tetikleyen en önemli olay internetin ortaya çıkışı olarak değerlendirilmektedir[87]. Günümüzde birçok iş ve işlem bilişim sistemleri ve internet üzerinden yürütülmekte ve sağlanmaktadır. İnternet ve bilişim sistemleri aracılığıyla yürütülen bu faaliyetlerin içerisine; kişisel iletişim, dijital bankacılık, online alışveriş gibi kişisel kullanımlarla birlikte, özel şirketlerin ve devletlerin yürütmüş olduğu büyük çaplı projeler de girmektedir. Bu durumun bir sonucu olarak internet ve bilişim sistemi güvenliğinin sağlanmasının önemi her geçen gün daha da artmaktadır. Kullanım alanı genişledikçe ve yaygınlığı arttıkça da bilişim suçlarının işleniş yoğunluğu ile sayısı giderek artmaktadır. İnternet güvenliğini tehlikeye atan ve yaygın görülen uzaktan erişim, kötü amaçlı yazılımlar, zararlı reklamlar, fidye yazılımları, botnetler (Kötü amaçlı yazılımlarla cihaza bulaştırılan ve izinsiz otomatik görevler yürüten bilgisayar ağları - robot ağı), paket korsanlığı, sahte Wi-Fi ağları, kimlik avı saldırıları gibi tehditler sıkça kullanıcıları hedef almaktadır[88]. Bunlar arasında özellikle, yanıltıcı e-postalar gönderilerek e-posta alıcısının kişisel bilgilerine ulaşmak veyahut zararlı

[83] "IP (İnternet Protokolü) Nedir?" (E. T. 15.01.2025) https://turk.net/blog/ip-internet-protokolu-nedir/#:~:text=IP%20adresleri%2C%20internete%20ba%C4%9Flanmak%20isteyen,siber%20g%C3%BCvenlik%20konular%C4%B1nda%20da%20kullan%C4%B1l%C4%B1r.
[84] "IP Adresi nedir?" (E. T. 15.01.2025) https://www.kaspersky.com.tr/resource-center/definitions/what-is-an-ip-address.
[85] "IP (İnternet Protokolü) Nedir?".
[86] "IP Adresi nedir?"
[87] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı , "Dijitalleşen Dünyada", 6.
[88] "İnternet güvenliği: Nedir ve Çevrimiçiyken Kendinizi Nasıl Koruyabilirsiniz?", (E. T. 15.01.2025) https://www.kaspersky.com.tr/resource-center/definitions/what-is-internet-security.

yazılım indirmelerini sağlamak amacıyla yapılan, failler açısından ucuz ve kolay yollardan biri olduğu için uzun yıllardır popüler bir şekilde kullanılan ve en eski saldırı yöntemi olan kimlik avı saldırıları ön plana çıkan tehditlerdendir[89]. Siber suçlar yalnızca internet suçlarından oluşmasa da, internet, bu suçların işlenmesinde diğer araçlardan çok daha yaygın bir şekilde kullanıldığındandır ki; siber suçların çoğunluğu internet aracılığıyla gerçekleşmektedir[90].

1.4.3. Data (Veri)

Data (Veri) Türkçede birden farklı alanda kullanılmakla birlikte, bilişim alanındaki kullanımıyla TDK sözlüğünde; "*Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi.*" olarak tanımlanmaktadır[91].

AKSSS'nin tanımında "Computer Data" olarak ifade edilen bilgisayar verisi, yine bu sözleşmeye göre; "*Bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan uygun programlar da içinde olmak üzere, bir bilgisayar sisteminde işlenmeye uygun biçimdeki her türlü bilgi veya kavramlar.*"[92] olarak tanımlanmıştır. 5237 sayılı TCK'nın gerekçesinde ise bilişim sistemi içerisindeki bütün soyut unsurların veri kavramı kapsamı içinde olduğu ifade edilmiştir[93]. Bu kapsamda büyük ölçekte programlar ve yazılımlar; küçük ölçekte rakamlar, harfler ve özel simgeler veri kavramının içinde olup; kısaca sisteme girilip burada işlenen ve depolanan her tür değer veridir[94].

Veri bir başka anlatımda her türden bilginin sayısal kodlara dönüştürülmüş hali olarak ifade edilmektedir[95]. Bilgi hiyerarşisinde en alt düzeyde bulunan, tek başına anlam ifade etmeyen ham sembol ve gerçeklerdir[96]. Bu sayısal kodlar bilgisayarlar aracılığı ile depo edilerek gerek görüldüğünde tekrar kullanıcı tarafından okunabilecek hale getirilir. Veriler bilgisayarların varlık nedenidir ve veri kavramı, ceza hukukunda suçun

[89] "Nasıl Koruyabilirsiniz?".
[90] Turhan, "Bilgisayar Ağları ile", 26.
[91] TDK sözlük, (E. T. 15.01.2025), https://sozluk.gov.tr/
[92] "Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001", (E. T. 15.01.2025) https://www.coe.int/en/web/cybercrime/the-budapest-convention
[93] "Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu (1/593)"
[94] Akbulut, *Bilişim Alanında Suçlar,* 189.
[95] Dülger, *İnternet İletişim Hukuku,* 84.; Yenidünya ve Değirmenci, *Mukayeseli Hukukta,*49.
[96] Sümeyra Karipçin, "Türk Ceza Kanunu'nda Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244/1,2), (Yüksek Lisans Tezi, Selçuk Üniversitesi, 2019), 21.

konusunu teşkil etmesi yönünden önem arz eden bir kavram olarak karşımıza çıkmaktadır[97].

1.4.4. Bulut Bilişim

Bulut bilişim (Cloud computing), dış hizmet verenlerce sunulan bilişim teknolojilerine dair veri depolama, yedekleme, uygulama geliştirme gibi hemen hemen her türlü hizmetin, bu tür hizmete ihtiyaç duyan kurumlarca internet üzerinden alınmasını ifade etmektedir[98]. ABD Ulusal Standartlar ve Teknoloji Enstitüsü bulut bilişimi, oldukça az bir hizmet sağlayıcı etkileşimiyle ağ, sunucu, depolama, uygulama gibi bilişim kaynaklarının toplandığı havuza her an ve her yerden erişim sağlayan bir model olarak tanımlamaktadır[99]. 2007 yılının sonlarında ortaya çıkan bu teknoloji; internet ortamında mevcut bulunan uygulamaların "kullandıkça öde" mantalitesiyle kullanıcılar tarafından yalnızca kullandıkları hizmet birimi kadar ödemede bulundukları bir sanal hizmet ortamı oluşturan, kullanıcıların verilerini "bulut" sistemine taşıyarak istedikleri an bu verilere erişimlerini sağlayan, yeni bir bilişim teknolojisidir[100].

Veri merkezi olarak çalışan bulut bilişim birçok kişiye ait veriyi içinde barındırması, oldukça geniş nitelikte bilgi birikimi içermesi ve internet üzerinden bağlantı sağlanması nedeniyle dış tehditlerin hedefinde daha çok yer aldığından[101] ceza hukuku açısından da önem arz etmektedir. Bulut bilişimde yaygın güvenlik riskleri güvenilir olmayan programlama ara yüzleri, paylaşılan teknoloji zayıflıkları ve veri sızıntısı gibi problemler olup, CSA'nın 2013 raporuna göre veri kaybı ve ihlali en önemli problemler olarak belirlenmiştir[102].

1.4.5. Nesnelerin İnterneti (IoT)

[97] Dülger, *İnternet İletişim Hukuku,* 83.
[98]Özcan Rıza Yıldız, "Bilişim Dünyasının Yeni Modeli: Bulut Bilişim (Cloud Computing) ve Denetim", *Sayıştay Dergisi*, 74 (2009) 7.
[99] Metin Turan, *Bulut Bilişim*, (Ankara: Seçkin Yayınları, 2019), 72.
[100] Bkz: Işıl Karabey Aksakallı, "Bulut Bilişimde Güvenlik Zafiyetleri, Tehditler Ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi.", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 5/1 (2019), 9. https://www.researchgate.net/publication/334155099_BULUT_BILISIMDE_GUVENLIK_ZAFIYETLERI_TEHDITLER_VE_BU_TEHDITLERE_YONELIK_GUVENLIK_ONERILERININ_INCELENMESI
[101] Bkz: Türkay Henkoğlu ve Özgür Külcü, "Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme", *Bilgi Dünyası*, 14/1 (2013), 67 vd. https://bd.org.tr/index.php/bd/article/view/135/129.
[102]Detaylı bilgi için bkz: Aksakallı, "Bulut Bilişimde", 11.

"Internet of Things" teriminin Türkçe ifadesi olan nesnelerin interneti, veri transferi yapabilen ve günlük hayatta kullandığımız akıllı nesnelerin birbiriyle iletişimini sağlayarak senkronize bir şekilde çalışmasını sağlayan yeni bir teknoloji olarak karşımıza çıkmaktadır[103]. İnşaat, imalat, sağlık, ticaret ve bilişim sektörü gibi birçok alanda kullanılan bu teknoloji, verimliliği artırıp iş yükünü azaltmak gibi birçok fayda sağlamakla birlikte[104]; barındırdığı verinin büyüklüğü ile art niyetli kişilerin ilgisini cezbetmekte ve güvenlik açısından da dikkat edilmesi gereken yeni güvenlik açıkları oluşturmaktadır.

1.4.6. Siber Uzay

İnternetin sivil hayata açılarak yaygınlaşması ve getirdiği teknolojik yeniliklerle beraber, insanlığın ulaştığı kara, deniz, hava, uzay boyutuna ek "siber uzay" boyutu gündeme gelmiştir[105]. Bilgisayar ağlarının sanal dünyası ve internet vasıtasıyla girilen bilgi dünyası olarak görülen siber uzay terimi ilk kez 1982 yılında yayınlanan bir hikayede kullanılmıştır[106]. Siber uzay, bilgisayarlardan oluşan ve toplumun bilgisayarlar etrafında oluşturduğu, küresel olarak birbirine bağlı bilgisayar destekli, erişimli ya da altyapılı yapay ya da sanal gerçeklik dünyası olarak ifade edilebilir[107]. Siber uzay internetteki web siteleri, bulut depolama servisleri, çevrimiçi forumlar, sosyal medya platformları gibi dijital alanların tamamını ifade etmek için kullanılır[108]. Siber uzayın bilgisayarlar, internete erişim sağlayan araçlar ve elektronik cihazlardan oluşan fiziksel bileşenler ile bilgisayar ağları, ağ sistemleri ve internetten oluşan sanal bileşenler olmak üzere iki bileşenden oluştuğu ifade edilmektedir[109]. Hemen hemen aynı tarihsel süreci paylaşan internet ile siber uzay kavramlarının birbirini tamamlamakla birlikte; internetin, siber uzayın bir aracı olduğu ifade edilmektedir[110]. Günümüzde bireysel ve

[103] "Nesnelerin İnterneti (IoT) Nedir?" (E. T. 15.01.2025) https://www.gtech.com.tr/nesnelerin-interneti-iot-nedir/.
[104] "(IoT) Nedir?".
[105] Nagihan Gün, "Türk Ceza Hukukunda Bilişim Suçları", (Yüksek Lisans Tezi, Çankaya Üniversitesi, 2020), 87.
[106] Tabriz Raufoğlu, *Hukuki Yönleri ile Siber Alanda Yetki Sorunu*, (Ankara: Adalet Yayınevi, 2022), 21.
[107] Bkz: Gözüşirin, "Model Önerisi", 23.
[108] Bkz: Egemen Demirer, "Siber Uzay ve Siber Güvenlik Nedir?", (E. T. 15.01.2025), *Hukuk ve Bilişim*, https://www.hukukvebilisimdergisi.com/siber-uzay-ve-siber-guvenlik/.
[109] Gözüşirin, "Model Önerisi", 23.; Haydar Çakmak ve Korhan Demir, "Siber Dünyadaki Tehdit ve Kavramlar", İçinde *Terör & Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altınok, (Ankara: Barış Platin Kitabevi ,2009), 28.
[110] Raufoğlu, *Yetki Sorunu*, 22.

toplumsal bazda internet kullanımının yaygınlaşması, özel sektör, kamu kurumları ve altyapı sektörlerinde bilişim sistemlerinin kullanılması, siber uzayda tüm bileşenlerin birbiriyle bağlantılı olması ve yapılan saldırılarda anonim hareket fırsatı bulunması bilişim dünyası açısından büyük güvenlik açıkları barındırmaktadır[111].

1.5. Bilişim Suçları

İnsanlık tarihi açısından önemi sanayi devrimi ile mukayese edilen[112] bilişim teknolojilerinin ortaya çıkmasıyla birlikte, dünyada teknoloji ve bilgi çağı dönemi başlamıştır. Bilgisayar ve internet insanların günlük hayatını değiştirdiği gibi; bunların art niyetli kişilerce kötüye kullanılmasıyla beraber, ceza hukuku açısından da yeni suç tiplerinin ortaya çıkmasına sebep olmuştur. Bu konuda ilk başta klasik suçlarda metinlerin geniş yorumlanması gerektiği, bilgisayarların bir yenilik getirmediği ve getirilecek bir düzenlemenin bilgisayarların gelişimini engelleyeceği yönünde düşünceler olsa da; nicel değişiklik getiren bilgisayarların nitel farklılıklar ortaya çıkardığını ve bu sebeple yeni düzenleme yapılması gerektiğini düşünenler baskın çıkmış, bu şekilde aksi tutumun kanunilik ilkesi ve kıyas yasağına aykırılık oluşturmasının önüne geçilmiştir[113].

Bu suçlar ilk ortaya çıktığında geleneksel suçların bilgisayar ortamında işlenen hali olarak bakılırken, zamanla ve teknoloji ilerledikçe klasik suçların dışında, yeni suç tiplerini ve türlerini oluşturduğu ve bu suçlara karşı korumanın sağlanması amacıyla yeni düzenlemeler yapılması gerektiği gözlenmiştir[114]. Kişilik hakkı ihlalleri, bireylere ve kurumlara maddi zarar verilmesi, ticari sırların bilişim sistemleri aracılığıyla çalınması gibi durumların ortaya çıkmasıyla, devletlerin bu konuda önlem alması zaruri bir hal almış ve bu fiiller ceza hukukunda yaptırımlara bağlanmak suretiyle, bu alanda koruma sağlanmaya çalışılmıştır[115].

---

[111] Gün, "Bilişim Suçları", 90.
[112] Turhan, "Bilgisayar Ağları ile", 25.; Semih Dokurer, "Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri", *İnet-tr 2001* (2003), http://www.dokurer.net/files/documents/Bilisim_Suclari_2001.pdf, 1.
[113] Akbulut, "Bilişim Suçları", 552.
[114] Şahin Gökçearslan, "Bilişim Suçları ve Etik", *Eğitimde Bilişim Teknolojileri I-II*, B.5, Pegem Akademi Yayıncılık, 2016, https://www.researchgate.net/publication/321535645_Bilisim_suclari_ve_etik, 129.
[115] Akbulut, "Bilişim Suçları", 548.

Bu konuda adımlar atılırken ilk olarak bilişim suçlarının öncelikle mevzuatlarda yer alan klasik suçlar karşısındaki konumlarını belirlemeye yönelik incelemeler yapılmış, bu suçların klasik suçlar içerisinde yer alması mı yoksa bağımsız bir alan olarak değerlendirilmesi mi gerektiği konusunda tartışmalar gerçekleşmiştir. Yapılan klasik suç – bağımsız suç tartışmasının sonucunda doktrinde bir grup klasik suçların fiziksel gerçeklik dışında bilişim suçları ile derin bir farkının olmadığını, bu nedenle bilişim suçlarının klasik suçlar içerisinde yer alması gerektiğini savunurken; diğer bir grup sadece siber ortamda gerçekleşebilen suçların mevcut olduğunu ve bu şekilde yeni ihlal tiplerinin de zaman içerisinde ortaya çıkabileceğini, dolayısıyla da bu suçların ayrı kategoride yer alması gerektiğini ileri sürmüşlerdir[116]. Her iki görüş de farklı devletlerce kabul görmüş ve her ülke kabul ettiği görüş çerçevesinde mevzuatlarında düzenlemelerde bulunmuştur.

Bilişim suçlarına yönelik bu tarz tartışmaların ortaya çıkması bilişim suçlarının kendine özgü nitelikleri ve klasik suçlardan ayrılan önemli noktaları göz önünde bulundurulduğunda oldukça doğaldır. Bakıldığı zaman; bilişim suçlarının teknolojinin gelişimi ve yaygınlaşması ile bağlantılı gelişim göstermesi, devamlı değişen ve küreselleşmeyle paralel bir şekilde işlenme oranının artması, zaman ve mekândan bağımsız anlık gerçekleşen suçlar olmaları, suçtan zarar görenin kişi, kurum ve toplum olmak üzere değişkenlik gösterebilmesi, klasik suçlarla mücadele yöntemlerinin bu suçlarla mücadelede yetersiz kalması ve uluslararası işbirliğinin etkin bir şekilde sağlanmasını gerektirmesi, dijital delil süreçleri içermesi ve bu delillerin klasik suçlarda elde edilen delillerden farklılık arz etmesi, failleri açısından yüksek kazanç ve düşük yakalanma riski bulundurması ve mağdurlarının çoğu zaman şikâyete başvurmaması gibi bilişim suçlarını klasik suçlardan ayıran birçok önemli özellikler bulunmaktadır[117]. Kaldı ki; teknolojinin gelişimiyle suçta kullanılan sistemlerin değişmesi ve sürekli yeni suç işleniş şekillerinin ortaya çıkması gibi özellikleri bilişim suçlarının tanımlanmasında dahi tartışmalara yol açmaktadır. Aynı zamanda bilişim sistemleri üzerinden

[116] Ayrıntılı bilgi için bkz: Turhan, "Bilgisayar Ağları ile", 34-38.
[117] Ayrıntılı bilgi için bkz: Hüseyin Akarslan, Bilişim Suçları, (Ankara: Seçkin Yayınları, 2015) , 38-40.

gerçekleştirilen eylemin suç olup olmadığı geleneksel suçlardaki gibi siyah ve beyaz olarak ayırt edilememekte, daha çok gri bir alan oluşturmaktadır[118].

Bilişim suçlarının kanunlarda tam bir tanımlaması yapılmamakla birlikte, ülkelerin mevzuatlarında ve milletlerarası çalışmalarda söz konusu suçlara neden olan fiillerin belirlenmesi yoluna gidilerek bu suçlar yaptırıma bağlanmıştır[119]. Öğretide ise örneğin; herhangi bir suç elektronik ortamda işlenebiliyorsa ve işlendiğinde suç olarak nitelendirilebiliyorsa, bu tür suçların siber suç olduğunu ifade eden genel tarzda tanımlamalar yapıldığı gibi[120], farklı kıstaslar oluşturmak suretiyle de birçok farklı tanım yapılmıştır. Bu tanımlamalar oluşturulurken genellikle belli başlı değerlendirmeler etrafında bir şekillenme gerçekleştiği görülmüştür. Bu konudaki değerlendirmeler temelde üçe ayrılmış ve ilk görüştekiler bu suçları ekonomik suçlar içerisinde görenlerden oluşurken, ikinci grup bilgisayar teknolojisini bilen özel kişilerin gerçekleştirdikleri suçlar olarak görenlerden ve son olarak üçüncü grup bu suçların gelişen teknolojiye ayak uydurması açısından tüm boyutlarıyla değerlendirilmesi gerektiğini düşünenlerden oluşmuştur[121]. Öğretide bu suçlar farklı şekillerde kategori edilmeye çalışılmış, bazı yazarlar bu suçları sadece bilgisayarlar vasıtasıyla malvarlığına karşı işlenen suçlar olarak değerlendirirken, diğer bazı yazarlar ise daha geniş bir çerçevede görerek bilişim sistemlerinin her tür kötüye kullanımından kaynaklanan suçları bilişim suçu olarak değerlendirmişlerdir[122]. Ancak sonuç olarak, hangi eylemlerin bilişim suçu oluşturduğu hangilerinin oluşturmadığı yönünde kesin bir ayrıma gidilemediğinden[123], genel çerçevede kabul gören bir tanımlama yapılması mümkün olmamıştır[124]. Bu durumun temel nedeni bilişim suçlarının üst düzey bir nitelik arz etmesi ve teknik gelişmelerin yoğunluğu sebebiyle de sürekli olarak yeni yeni suç işleniş şekillerinin ortaya çıkması olarak görülmektedir[125].

---

[118] Furkan Yılmaz ve Fuat Güllüpınar, "Türkiye'de Bilişim suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi", *Uluslararası Toplum Araştırmaları Dergisi*, 15/10 (2020), 5374.
[119] Akbulut, "Bilişim Suçları", 549.
[120] Özüdoğru, "Mücadele Yöntemleri", 9.
[121] Pallı, "Hukukta Bilişim Suçları", 40.
[122] Ersoy, "Hukuki Koruma Çerçevesinde", 159.
[123] Dülger, *İnternet İletişim Hukuku*, 81.
[124] Karagülmez, *Bilişim Suçları,* 59.
[125] Dülger, *İnternet İletişim Hukuku*, 81.

Teknoloji alanındaki gelişmenin hızla sürmesi ile bu alanda işlenen hukuka aykırı eylemlerin istatiksel olarak ifade edilmesindeki ve gerçek zararın belirlenmesindeki sıkıntılardan dolayı, bilişim suçlarının yeterli görülen bir düzeyde çerçeve içerisine alınamadığından bu suçlara "çizgisiz çerçeveli suçlar" da denmektedir[126].

Bilişim suçlarının tanımlamasında yaşanan bu zorluk sebebiyle öğretide birçok farklı ölçüt esas alınarak bilişim suçları belli bir çerçeve içine alınmaya çalışılmış ve farklı yazarlarca bu konuda farklı ölçütler getirilmiştir. Bu ölçütler temelde; bilgisayarın amaç veya araç olarak kullanımını esas alan, bilişim sistemleri ile bağlantılı suçları esas alan, bilişim suçlarını malvarlığı ihlalleriyle sınırlandıran, bilgisayar kullanımını esas alan, faili esas alan ve veri iletişim ağlarını esas alan[127] ölçüt olmak üzere 6 farklı şekilde karşımıza çıkmaktadır.

Bilgisayarın amaç veya araç olmasını arayan görüşte, mevzuatta suç olarak düzenlenmiş fiillerin yanında, suç olarak henüz düzenlemesi yapılmamış ancak yaptırım altına alınması gereken bilgisayar manipülasyonu, bilgisayar casusluğu, bilgisayar sabotajı ve zaman hırsızlığı, hardware ve software hırsızlığı gibi fiillerin de bu kapsamda suç olduğunu savunmakta ve bilgisayarın fiilin icrası için araç olduğu tüm bu fiilleri de kapsam içine almaktadır[128]. Ancak bu görüş bilgisayara mahsus olmayan (örneğin klasik hırsızlık suçunun konusunu oluşturacak hardware gibi parçaların çalınması gibi) fiilleri de içerdiği için eleştirilmiş; görüşün sebep olduğu bu problemi ortadan kaldırmak için, bu görüşün savunucularından bazıları, fiilin elektronik veri işlemleriyle sınırlandırılması gerektiğini savunmuşlardır[129].

Bilişim sistemleri ile bağlantılı suçları esas alan görüşte bilişim sistemleri kullanılarak işlenen her tür fiil bilişim suçu olarak kabul edilmektedir ve bu kapsamda mağdur veya mağdurların zarar gördüğü veya görme ihtimalinin mevcut olduğu fiillerin tamamını kapsamaktadır[130]. Bu görüş bilişim suçlarını çok geniş bir hale getirdiği ve genel suç tiplerinden ayırma imkânı bırakmadığı için eleştirilmiş; eleştiriler sonucu, bilgisayar

[126] Altunok, "Bilişim Suçları", *Denetişim Dergisi*, 8(2011), 76.
[127] Akbulut, *Bilişim Alanında Suçlar*, 59 vd.
[128] Akbulut, *Bilişim Alanında Suçlar*, 59-61.
[129] Akbulut, *Bilişim Alanında Suçlar*, 61.
[130] Pallı, "Hukukta Bilişim Suçları", 41.

yerine başka bir araç getirildiğinde fiil işlenemiyorsa bilişim suçu olması gerektiği konusunda görüş daraltılmıştır[131].

Bilişim suçlarını malvarlığı ihlalleri ile sınırlayan görüşte ise özel hayatın korunması gibi kişilik hakları ihlalleri bilişim suçu olarak görülmemekte ve bu açıdan da kişilik hakkı ihlalleri de bilişim sistemleri aracılığıyla gerçekleştiriliyorsa bilişim suçu oluşturması gerektiği gerekçesiyle öğretide yetersiz bulunarak eleştirilmektedir[132].

Bilgisayar kullanımını esas alan görüşte ise, bilgisayar kullanımı bu suçların zorunlu unsuru olarak kabul edilmekle birlikte[133] günümüz koşullarında bu suçların oluşabilmesi için yalnızca bilgisayarların temel alınmasının geçerliliğinin kalmadığını belirtmek gerekir. Bu görüşe karşı olanlar da benzer çerçevede bu suçların başka cihazlarla ya da başka cihazlara karşı da işlenebileceğini ve bu suçlara yönelik olarak TCK'daki kavram kullanımının da bu suçları bilgisayarla sınırlandırmamak amacı güttüğünü ifade etmişlerdir[134].

Veri iletişim ağlarını esas alan görüşte adından anlaşılacağı üzere bilgisayar ağları temel alınmakta; faili esas alan görüşte ise failin bilgisayar bilgisine göre bir değerlendirme yapılarak yalnız bu konuda bilgili olan kişilerin bu suçları işleyebileceği savunulmaktadır[135].

Görüldüğü üzere doktrinde bu suçları belirlemeye ilişkin birçok ölçüt ortaya atılmış[136], ancak bu ölçütlerin hiçbiri bilişim suçlarını tam olarak ifade edemediğinden[137], bu suçları oluşturan fiillerin neler olduğu belirlenerek mevzuatlara yansıtılması daha yerinde görülmüştür.

Avrupa Ekonomik Topluluğu bir tavsiye kararında bilişim suçlarını şu şekilde 5'e ayırarak incelemiştir: "*Bilgisayardaki kaynağa yasadışı olarak ulaşarak transferini sağlamak için bilgisayar verilerine girmek, bu verileri bozmak, silmek, yok etmek; sahtekarlık amacıyla kasten bilgisayar verilerine veya programlarına girmek, bozmak,*

[131] Akbulut, *Bilişim Alanında Suçlar*, 64.
[132] Akbulut, *Bilişim Alanında Suçlar*, 63.
[133] Akbulut, *Bilişim Alanında Suçlar*, 64.
[134] Pallı, "Hukukta Bilişim Suçları", 43.
[135] Akbulut, *Bilişim Alanında Suçlar*, 64-67.
[136] Bu konuda ayrıntılı bilgi için bkz: Akbulut, *Bilişim Alanında Suçlar*, 59 vd.
[137] Dülger, *İnternet İletişim Hukuku*, 82.

silmek, yok etmek; bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek; ticari manada yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak; bilgisayar sistemi sorumlusunun izni olmaksızın, konulmuş olan emniyet tedbirlerini aşmak suretiyle sisteme kasten girerek müdahalede bulunmak"[138].

Doktrinde ise bu konuda birçok farklı sınıflandırma yapıldığı görülmektedir.[139] Bunlardan birinde bilişim suçları; bilişim sistemine karşı işlenen fiiller ve bilişim sistemi aracılığıyla işlenen fiiller olmak üzere ikiye ayrılmaktadır[140].

İkinci bir sınıflandırmaya göre bilişim suçları üçe ayrılmış ve ilk olarak bilişim sistemlerinin veya içerdiği verilerin bütünlüğüne ve güvenliğine karşı işlenen suçlar, ikinci olarak bilişim sistemlerinin kullanımının nitelikli hal olduğu suçlar, son olarak da bilişim sistemlerinin araç olarak kullanıldığı ancak suçun unsurunu oluşturmadığı suçlar olarak değerlendirilmiştir[141].

Üçüncü bir sınıflandırmaya göre ise; bilgisayarın fiziksel yapısına yönelik fiziksel olarak gerçekleştirilen eylemler, bilgisayarın tek başına çalışma sistemine ilişkin elektronik alanı hedef alan eylemler ve internet ortamında gerçekleştirilen eylemler olmak üzere üçe ayrılarak incelenmiştir[142].

Birleşmiş Milletler 1994'te çıkarmış olduğu rehberde yaygın işlenen bilgisayar suçlarını; "bilgisayar veri ve/veya programlarının değiştirilmesi ya da hasara uğratılması, bilgisayar manipülasyonu ile dolandırıcılık, bilgisayar sahteciliği, bilgisayar sistem ve servislerine yetkisiz erişim, yasal olarak korunan programların izinsiz çoğaltılması" olmak üzere 5 kategoriye ayırmıştır[143]. İtalya'da 2000 yılında düzenlenen "The Challenge of Borderless CyberCrime" panelinde ise bilişim sistemleri üzerinden gerçekleştirilen yetkisiz giriş, hukuka aykırı kullanım, veri değişimi, tahribi,

---

[138] Altunok, "Bilişim Suçları", 77.
[139] Bu konuda ayrıntılı bilgi için bkz: B. Zakir Avşar ve Gürsel Öngören, *Bilişim Hukuku*, (İstanbul: Türkiye Bankalar Birliği, 2010), 123 vd.
[140] Avşar ve Öngören, *Bilişim Hukuku,* 123.; Haluk İnanıcı, "Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü", *İstanbul Barosu Dergisi,* 70/7,8,9 (1996) : www.inanici-tekcan.av.tr/images/pdf/bilisim-yazilim.pdf , 3.
[141] Dülger, *İnternet İletişim Hukuku*, 82.
[142] Karagülmez, *Bilişim Suçları,* 71.
[143] Özüdoğru, "Mücadele Yöntemleri", 10.

ele geçirilmesi ve sahtekârlık gibi bazı fiillerin üye ülkelerce cezai yaptırıma bağlanması tavsiye edilmiştir[144]. Bilişim suçlarını sınıflandırırken ise; hacking, verilere yönelik suçlar, bilişim ağlarına yönelik suçlar, sanal tecavüz gibi fiilleri içermek üzere "Dar anlamda" ve bilişim ortamında cinayet, tehdit ve şantaj, hakaret ve sövme, taciz ve sabotaj, pornografi, röntgencilik, manipülasyon, dolandırıcılık, hırsızlık, sahtekârlık, sanal/siber terör gibi fiilleri içermek üzere "Geniş anlamda" siber suçlar olarak ikiye ayırmıştır[145]. Bu sınıflandırmada göze çarpan dar anlamda bilişim suçlarının sisteme yönelik fiiller olmasıyken; geniş anlamda bilişim suçlarının sistem aracılığıyla işlenen fiilleri içermesidir.

Görüldüğü üzere; şiddete dayanmayan suçu ifade eden bir kavram olan "Beyaz Yaka Suçu" kapsamında da değerlendirilen[146] bilişim suçları ile ilgili olarak ulusal ve uluslararası hukuk çerçevesinde birçok farklı tanımlama ve sınıflandırmanın yapıldığı görülmektedir. Bu noktada tanımlama ve sınıflandırma yapılırken önemli olan, bilişim suçlarının gelecek yeni suç işleme yöntemlerini ve fiilleri kapsayacak şekilde düzenlenmesi gerektiği, ancak bu durumun kanunilik ilkesini aşmayacak düzeyde tutulması gerekliliğidir.

Yine bu suçları tanımlanırken önem arz eden başka bir husus da; bu suçların aslında her ne kadar bilişim sistemleri üzerinden işleniyor olsalar da asıl hedefin daima bu sistemlerdeki verileri ya da sistemin işleyişini hedef almasıdır[147]. Aksi halde, doğrudan bilişim sisteminin donanımını hedef alan bir fiil bu noktada bilişim suçlarına değil; mala zarar verme, hırsızlık gibi diğer suçların konusunu oluşturacak ve bu suçlara mevcudiyet verecektir[148].

Bilişim suçlarının tanımlanmasında yaşanan zorlukların yanında, bu suçların soruşturma ve kovuşturmasında yaşanan zorluklar da oldukça dikkat çekicidir. Bu suçların özel yetenek ve teknik bilgi gerektiren suçlar olmaları (Bu özelliği aynı zamanda bilişim suçlarını klasik suçlardan ayrılan önemli özelliklerinden biri olarak da karşımıza

[144] Pallı, "Hukukta Bilişim Suçları", 68.
[145] Altunok, "Bilişim Suçları", 77. B. Zakir Avşar ve Gürsel Öngören, *İnternet Hukuku,* (Ankara: TOBB Yayınları, 2009), 96 vd.
[146] Hasan Dursun, "Bilgisayar İle İlgili Suçlar", Yargıtay Dergisi, 24/3, (1998): 334.; İnanıcı, "Uygulama İçinden Görünüşü", 2.
[147] Dülger, *İnternet İletişim Hukuku,* 82.
[148] Dülger, *İnternet İletişim Hukuku,* 82.

çıkmaktadır[149]) ve genellikle bilişim alanında uzman kişiler tarafından işlense de, düşük seviyede teknik bilgi sahibi olan insanlar tarafından işlendiğinde de büyük zararlara neden olabilmesi[150] bu zorluklardan bazılarıdır. Yine; bu suçların bilişim sistemlerinde yer alan soyut bir nitelik arz eden veriler üzerinde gerçekleştirilmesinden kaynaklı olarak faillerinin yakalanması oldukça zordur[151]. Tüm bu tanımlamaya ve kovuşturmaya yönelik zorluklar bilişim suçlarını oluşturan fiillere yönelik gerekli olan korumanın ciddiyetini artırmakta ve bu suçları üzerinde durulması gerektiren önemli bir noktaya getirmektedir.

1.5.1. Tarihsel Açıdan Bilişim Suçlarına Bakış

Teknolojinin suça konu edinmesi yalnızca günümüz şartlarında değil, tarih sahnesinde çok eski zamanlardan beri söz konusu olmuştur. Ortaya konan neredeyse her yeni buluş zaman içinde art niyetli kişilerce kötüye kullanım yolları keşfedilerek suça bir şekilde aracılık etmiştir. Bunun bir örneği 19. Yüzyılda telgraf sistemleri üzerinden dolandırıcılık faaliyetlerinin gerçekleştirilmesi olarak gösterilebilir[152]. Bu dolandırıcılık modeliyle günümüz bilişim sistemleri üzerinden işlenen fiiller arasında teknolojinin oluşturduğu güveni kötüye kullanma noktasında oldukça benzerlik olduğu görülür[153].

1801'de Fransa'da J.M. Jacquard'ın özel kumaşların dokunmasında kullanılmak üzere ürettiği otomatik delikli kartların kendi işlerini tehlikeye attığını düşünen işçiler tarafından sabote edilmesi ile kullanılmaktan vazgeçilmesinin ilk bilişim suçu olduğu kabul edilse de[154], teknik anlamda bilişim suçlarının ortaya çıkışı 1960'lı yılların sonunda kişisel verilerin topluca saklandığı veri bankalarının oluşturulmasıyla beraber bu konuda veri güvenliğine karşı tehditlerin başlamasıyla gündeme gelmiştir[155]. Bu suçların ilk dünyaya duyuruluşu 1966'da Minneapolis Tribune gazetesi aracılığı ile olmuştur[156]. ABD'de gerçekleşen bu olayda bir şirkette programlama işiyle uğraşan bir kişi banka programının mevcuttan fazla para çekimlerini tespit ederek özel bir protokole

[149] Durmuş Tezcan, Mustafa Ruhan Erdem ve Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku*, (Ankara: Seçkin Yayıncılık, 2023), 1026.
[150] Akarslan, *Bilişim Suçları*, 38.
[151] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1026.
[152] Dülger, *İnternet İletişim Hukuku,* 101.
[153] Dülger, *İnternet İletişim Hukuku,* 101.
[154] Pallı, "Hukukta Bilişim Suçları", 45.
[155] Altunok, "Bilişim Suçları", 76.
[156] Dülger, *İnternet İletişim Hukuku,* 104.

geçiren kısmını kendi hesabına gönderecek şekilde ayarlayarak bu paraları 4 ay boyunca kendi hesabına yönlendirmiş ve bu olay bilinen ilk bilişim suçu olarak kayıtlara geçmiştir[157].

1970'lerde "phreaker" olarak adlandırılan ve telefon sistemlerine girerek ücretini ödemeden telefon görüşmeleri yapan hackerlar ile bilişim suçları duyulmaya başlanmış[158]; 1970'li yıllarda ağların kullanımı hacking fiillerini yaygınlaştırmış; 1980'lerde ise PC'lerin yaygın bir şekilde kullanılmaya başlamasıyla program korsanlığı fiillerinde artış olmuş[159], bilişim suçlarında nitelik olarak değişimler görülmüş ve yalnızca malvarlığı değerlerine yönelik suçlar olmadıkları, kişisel veriler gibi diğer hukuki değerlere karşı da bu tarz suçların işlenebileceği ortaya çıkmıştır[160]. Bilgisayarları modemlerle birbirine bağlayan BBS (Bulletin Board System) ağlarının yaygınlaşması dünya genelinde bilgisayarları birbirine bağlamış; yeni nesil antisosyal tavırlar sergileyen, sistem dosyalarını yok edip web sitelerini ele geçiren saldırgan tiplerini ve modern saldırı araçlarını ortaya çıkarmıştır[161]. Yine 1980'lerde ATM'lerin ortaya çıkışıyla banka kartlarına ilişkin suçlar da ortaya çıkmıştır[162]. Ancak tüm bunlarla birlikte bilişim suçlarında asıl patlama 1990'larda internetin ortaya çıkışı ile birlikte meydana gelmiş ve internetin yaygınlaşmasıyla bu alanda suçlar her yıl giderek artmıştır[163].

Kişisel bilgisayarların ve internetin gelişimi ile internet üzerinden gerçekleştirilen hukuka aykırı eylemlerin sayısı giderek çoğalmış ve bu durum hukuk sistemlerinin bu konu üzerine eğilimini arttırmıştır. Bilişim sistemlerine ilişkin hukuka aykırı eylemlerin artmasında önemli dönüm noktalarından biri bilgisayar solucanlarının ortaya çıkmasıyla olmuştur[164]. Bu konuda yargı önüne gelen ilk dava Robert T. Morris'in geliştirmiş olduğu ilk bilgisayar solucanı Morris Worm ile birlikte altı bin bilgisayarı etkileyerek zarara yol açması ile ortaya çıkmıştır[165]. Bu davada Morris ABD'de Bilgisayar

[157] Akbulut, *Bilişim Alanında Suçlar,* 51.
[158] Gümüş, "Polisin Eğitimi", 44.
[159] Altunok, "Bilişim Suçları", 76.
[160] Akbulut, *Bilişim Alanında Suçlar*, 52.
[161] Gümüş, "Polisin Eğitimi", 44.
[162] Altunok, "Bilişim Suçları", 76.
[163] Akbulut, *Bilişim Alanında Suçlar*, 53.
[164] Saltuk Buğra Solmaz, "Siber Güvenlik Tarihindeki Dönüm Noktaları: Tehditlerin Evrimi ve Savunma Stratejileri", *Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve Uygulama Merkezi Dergisi*, 3/1, (2023): 2.
[165] Dülger, *İnternet İletişim Hukuku,* 104.

Sahtekarlığı ve Kötüye Kullanımı Kanunu olan United States Code 18'i ihlal ettiği gerekçesiyle yargılanmış ve dava Morris'in hapis cezasına ve tazminata çarptırılmasıyla sonuçlanmıştır[166]. Yine aynı dönemde Condor lakabıyla bilinen Kenvin Mitnick sistemlere girerek gizli bilgi ve kredi bilgisi çalma, motor araçları veri tabanına girme ve hub'ları uzaktan kontrol etmekle suçlanarak devlet bilişim sistemine suç amaçlı giren ve FBI'ın en çok arananlar listesinde yer alan ilk saldırgan olmuştur[167]. 2000'li yıllarda ise özellikle veri ihlalleri ve fidye yazılımlarda büyük artış olurken, buna ilişkin en büyük örneklerden biri de 2017'de büyük çoğunlukla Avrupa ülkelerinde etki gösteren ve birçok bilgisayarı etkileyerek bu tarz güvenlik açıklarının global anlamda sarsıcı etkileri olabileceğini kanıtlayan WannaCry saldırısı olmuştur[168]. Bilişim suçları ifadesinin yaygın bir biçimde kullanılmaya başlaması ve öğrenilmesi ise bilimsel dergilerin bu konuyu ele alması, bu dergilerde yazılar yazılması ile söz konusu olmuş ve bunun sonucunda toplumun bilişim sistemlerinin zayıflıklarını görmesiyle kavramın yaygınlaşması sağlanmıştır[169].

Hukukun asıl amacının özgürlükleri teminat altına alınması olduğu, amacın özgürlükleri kısıtlamak olmadığı gözetildiğinde, bir konunun hukuk kuralları kapsamına alınmasında öncelikle bu durumun sosyal bir zorunluluk haline gelmiş olması şart olup, ceza kanunlarının sınırlandırıcı yapısı da göz önünde bulundurulduğunda, zaruri hale gelmedikçe bir konuda cezalandırma mümkün olmadığından, hukukun toplumu ve teknolojiyi geriden takip eden bir özellik taşıdığı görülmektedir[170]. Bu durumun somut örneklerinden biri de bilişim suçlarının düzenlenmesinde görülmüştür.

Bilişim suçları günümüzde en çok internet üzerinden gerçekleştirilmekle birlikte bilişim korsanlığı, kişisel verilere karşı suçlar, bilişim sistemleri vasıtasıyla hukuka aykırı ekonomik çıkar elde etme ve organize suç örgütleri ile terör örgütleri için propaganda aracı olarak kullanılmasıyla siber terörizm yaygın olarak görülmektedir[171]. Bilişim suçlarının geleceği ise geçmişten günümüze teknolojinin evrimiyle paralel bir gelişme gösterdiğinden, günümüzde sanal gerçeklik, sürücüsüz araçlar, yapay zekâ gibi

[166] USCA, 07.03.1991, 774. https://scholar.google.com/scholar_case?case=551386241451639668
[167] Gümüş, "Polisin Eğitimi", 45.
[168] Solmaz, "Tehditlerin Evrimi", 3.
[169] Dülger, *İnternet İletişim Hukuku*, 103.
[170] Ekici, "İnternetin Regülasyonu", 28.
[171] Dülger, *İnternet İletişim Hukuku*, 104-106.

gelişmelerin ileride varacağı nokta bilişim suçlarının da geleceğini belirleyecek ve ceza hukukunda yansımasını gösterecektir[172].

Bilişim suçlarına ilişkin ilk düzenlemeler ise, bu suçun ilk ortaya çıktığı yer olan ABD'de görülürken[173] 1970'lerde Avrupa'da bu konu üzerine tartışmalar yeni yeni yapılmaya başlamış, 1970'lerin sonlarına doğru ortaya çıkan ilk kriminolojik çalışmalar bilişim suçlarını sınırlı bir miktarda ele almış, tüm suçları kapsamamıştır[174]. Bilişim suçlarına ilişkin ilk düzenlemelerin yapıldığı ABD'de suçlar öğretide; veri veya hizmet hırsızlıkları, mülkiyet hırsızlıkları, giriş ihlalleri, veri sahtekarlığı, şahıslardan kaynaklı hatalar, gasp, sır aleyhine ihlaller, sabotajlar, maddiyata yönelik hırsızlıklar, vakalarda gerçekleştirilen sahtekarlıklar, ATM kartı konusunda hırsızlıklar, manyetik kartlarının şifrelerine karşı gerçekleştirilen eylemler olmak üzere 12 başlıkta değerlendirilmiştir[175].

1990'lı yılların sonlarına doğru internetin kullanıcı sayısının artmasıyla hukuka aykırı içeriklerin artması, ulusal ve uluslararası hukukta bilişim suçlarına ilişkin ciddi adımlar atılmasına ve bu konuya ilişkin düzenlemeler yapılmaya çalışılmasına zemin hazırlamış; nihayetinde Avrupa Konseyi'nin bu konuya el atmasıyla, 23 Kasım 2001'de Avrupa Konseyi Siber Suç Sözleşmesi imzalanarak yürürlüğe girmiştir[176]. Avrupa Birliği ile Birleşmiş Milletler Komisyonu'nun hazırladığı ortak raporda bilişim alanında suçlar; bilgisayar sistemleri ve servislerine yetkisiz erişim ve dinleme, bilgisayarların sabote edilmesi, bilgisayar aracılığıyla dolandırıcılık, bilgisayar kullanılarak sahtecilik, kanun tarafından korunan bir yazılımın izin alınmadan kullanılması, kanuna aykırı yayınlar olmak üzere 6 ana bölümde değerlendirilmiştir[177].

Türk mevzuatında ise bilişim suçları ile ilişkin ilk düzenlemeler Fransa'da Godfrain Kanunu olarak bilinen 5 Ocak 1988 tarihli Bilişim Sahtekârlığına İlişkin Kanun örnek alınarak hazırlanmıştır[178]. 1989 yılına kadar ceza hukukumuzda bilişim kavramına herhangi bir yer verilmemiştir[179]. 765 sayılı eski TCK'nın 1987'de tamamlanan ön

[172] Akbulut, *Bilişim Alanında Suçlar*, 54.
[173] Fatih Selami Mahmutoğlu, "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu", *Journal of Istanbul University Law Faculty,* 59/1-2 (2011): 41.
[174] Dülger, *İnternet İletişim Hukuku,* 103.
[175] Altunok, "Bilişim Suçları", 76. Avşar ve Öngören, *İnternet Hukuku*, 96.
[176] Dülger, *İnternet İletişim Hukuku*, 105.
[177] Altunok, "Bilişim Suçları", 77.
[178]Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1024. Yazıcıoğlu, "Yeni Türk", 102.
[179] Apaydın, *Bilişim Ceza Hukuku*, 152.

tasarısında bu suçlara ilişkin bir düzenleme bulunmazken[180], 1989 tarihli ön tasarıda bilişim alanının tarifi yapılmış[181], "topluma karşı suçlar" başlığı altında beş maddeden oluşan bir düzenleme öngörülmüştü[182]. Bu konuda ilk düzenleme ise 1991'de 3756 sayılı Kanun ile 765 sayılı eski TCK'ya bilişim suçlarına ilişkin yeni maddeler eklenmesi suretiyle olmuştur[183]. 1989 tarihli TCK ön tasarısında yer alan bilişim alanına ilişkin tanım aynı şekliyle 765 sayılı eski TCK'ya 3756 sayılı Kanun ile getirilen değişikliğin gerekçesinde de kullanılmıştı[184]. Bu düzenlemede bilişim suçlarını içeren 11. bölümün başlığı "Bilişim Alanında Suçlar" olarak ifade edilmiş olsa da ilgili maddelerde bilişim terimi kullanılmamış, bilişim ifadesi yalnızca başlıkta yer almıştır[185]. Bu bağlamda 765 sayılı eski TCK'da yapılan değişiklikle bilgileri otomatik işleme tabi tutulmuş bir sistemle ilgili olarak ele geçirme ve tasarruf suçu m. 525/a'da, tahrip, bozma ve yarar sağlama suçu m. 525b'de, delil tahrifi m. 525c'de ve m. 525/a-b açısından fer'i ceza m. 535/d'de düzenlenmiştir[186].

1995'te 4110 sayılı Kanun ile 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda bazı değişikliklere gidilerek bilişim yazılımları ve veriler "eser" olarak değerlendirilmiş[187], 2004'te 5070 sayılı Elektronik İmza Kanunu ile yeni suç tipleri düzenlemesi gerçekleşmiş, yine aynı yıl çıkarılan 5237 sayılı TCK'da bu suçlar ayrıntılı olarak düzenlenmiştir[188].

2013 yılında 7258 Sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkındaki Kanun'a internet üzerinde yapılan bahis oyunlarına ilişkin düzenleme getirilerek yurtdışı bahis sitelerine erişim sağlama imkanı sağlamak suç haline getirilmiştir[189]. 2007 yılına gelindiğinde ise yapılan bir dizi düzenlemeyle

[180] Gülennur Erkan, "Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları", (Yüksek Lisans Tezi, Erciyes Üniversitesi, 2021), 36. Olgun Değirmenci, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", *TBB Dergisi*, 58 (2005), 197.
[181] Apaydın, *Bilişim Ceza Hukuku,* 152.
[182] Erkan, "Bilişim Sistemine", 36.
[183] Dülger, *İnternet İletişim Hukuku*, 106. Soyaslan, *Özel Hükümler*, 634.
[184] Apaydın, *Bilişim Ceza Hukuku,* 152.; Yenidünya ve Değirmenci, *Mukayeseli Hukukta*,28.
[185]Erkan, "Bilişim Sistemine", 36.
[186]Bkz: Ö. Umut Eker, ""Türk Ceza Hukuku'nda Bilişim Suçları"" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", *Türkiye Barolar Birliği Dergisi*, 19/62 (2006): 111 vd.
[187]Erkan, "Bilişim Sistemine", 39.
[188] Dülger, *İnternet İletişim Hukuku*, 106.
[189] Necmettin Yazıcı, "Türk Ceza Hukukunda Bilişim Suçları (TCK M. 243-244 ve 245)", (Yüksek Lisans Tezi, Fatih Sultan Mehmet Vakıf Üniversitesi, 2021), 39.

internet kişilerinin sorumlulukları belirlenmiş, sonrasında TTK, TBK, HMK ve TCK'da konuya ilişkin düzenlemeler yapılmaya devam edilmiştir[190]. Yine 2007 yılında internet sistemleriyle ilgili ilk özel yasal düzenleme olan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun çıkarılarak internet içerik sağlayıcılarının yükümlülük ve sorumlulukları düzenlenmiş, bu kanunda TCK'da düzenlenen bazı suç maddelerine yollama yapılmak suretiyle, sayılan suçların oluştuğu hususunda yeterli şüphe oluşması halinde içeriğin çıkarılması ya da erişimin engellenmesi hususları düzenlenerek meydana gelebilecek hukuka aykırılıkların önüne geçilmek istenmiştir[191]. 10 Kasım 2010'da ise AKSSS imzalanmış ve 22 Nisan 2014 tarihinde onaylanarak hukukumuzun bir parçası haline gelmiştir[192]. 24 Mart 2016'da ise 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilmiş ve yürürlüğe girmiştir.

1.5.2. Kavramsal Açıdan Bilişim Suçları

Bilişim suçları Amerika'da ilk ortaya çıktığında computer related crime[193] (bilgisayar bağlantılı suç), crimes against computer (bilgisayara karşı işlenen suçlar), computer assisted crime (bilgisayarla işlenen suç)[194] olarak çeşitli şekillerde ifade edilirken günümüzde daha çok computer crime (bilgisayar suçu) ve cybercrime (siber suç) ifadeleriyle adlandırılmaktadır[195].

Türkiye'de ise öğretide bu konuda birçok farklı adlandırma yapıldığı ve bir görüş birliğine varılmadığı görülmektedir[196]. Bilişim suçları; bilişim suç hukuku[197], bilgisayar ile ilgili suç[198], bilişim alanında işlenen suç, bilgisayarlara karşı işlenen suç, bilgisayarlar aracılığıyla işlenen suç[199], bilgisayar suçu[200], siber suç[201], sanal suç[202],

[190] Dülger, *İnternet İletişim Hukuku,* 106.
[191] Yazıcı, "Bilişim Suçları", 37.
[192] Dülger, *İnternet İletişim Hukuku*, 106.
[193] Yılmaz Yazıcıoğlu, *Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle*, (İstanbul: Alfa Yayınları, 1997), 126.
[194] Yenidünya ve Değirmenci, *Mukayeseli Hukukta,* 30.
[195] Dülger, *İnternet İletişim Hukuku,* 77.
[196] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku,* 1024.
[197] İnanıcı, "Uygulama İçinden Görünüşü", 3.
[198] Dursun, "Bilgisayar İle İlgili Suçlar", 334.
[199] Dülger, *İnternet İletişim Hukuku,* 78.
[200] Faruk Erem, "Bilgisayar Suçları ve Türk Ceza Kanunu", *İstanbul Barosu Dergisi*, 19/10-11-12 (1993): https://tbbdergisi.barobirlik.org.tr/m1993-19932-968, 178.

internet suçu[203], bilişim sistemi aracılığıyla işlenen suç[204], teknoloji suçu, ileri teknoloji suçu[205], bilgisayar bağlantılı suç, elektronik suç[206] gibi birçok şekilde ifade edilmektedir. Ancak bu ifadelerin birçoğu bu suçları tanımlamada yetersiz kalmaktadır.

"İnternet suçu" ya da "internet alanında suç" ifadesinin bu suçlarda yalnızca internet yoluyla işlenebileceği algısı oluşturduğundan, bu suçları tanımlamakta eksik kaldığı görülmektedir[207]. Her ne kadar internet bu suçların işlenmesine zemin hazırlayan geniş bir alan sunsa da, bunun dışında intranet ve extranet gibi ağların da bulunduğu ve bu ağlar aracılığıyla suç işlenebilmesinin de mümkün olduğu yönüyle eleştirilmiş, bu suçların işleniş ortamına göre adlandırılacak olması uygun bulunmamıştır[208]. Başka bir görüşe göre ise internet suçları bilişim suçlarından farklı bir nitelik arz etmekte, yalnızca internet ortamında işlenen suçları ifade etmektedir[209]. Buna göre; bu suçların işlenmesinde her ne kadar bilişim sistemleri aracılığıyla internete erişiliyor olsa da; bu suçlar bilişim suçlarını değil internet suçlarını oluşturmaktadır[210].

"İleri teknoloji suçu" ifadesi ileri teknoloji kavramının zamanla değişebileceği ve dolayısıyla ileride çok daha farklı teknolojilerin ortaya çıkmasıyla bugünün teknolojisinin eskide kalacak olması yönünden, ayrıca da bilişim sistemleriyle işlenen klasik suçları kapsamaması dolayısıyla bu suçları adlandırmada uygun olmadığı gerekçesiyle eleştirilmektedir[211].

"Bilgisayar suçu" ibaresi ise, bilişim sistemlerinin tamamını kapsamayıp, bu suçların yalnızca bilgisayarlar aracılığıyla işlenebileceği algısına sebebiyet verdiğinden, bu

---

[201] Servet Yetim, "Bilişim Suçları ve Etkin Mücadele Yöntemleri", Terazi Hukuk Dergisi, 9/95 (2014) : 81.; Kayıhan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", *Journal of Istanbul University Law Faculty*, 59/1-2 (2011): 3.
[202] Yılmaz Yazıcıoğlu, "Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı", İçinde *Uluslararası İnternet Hukuku Sempozyumu*, (İzmir: Dokuz Eylül Üniversitesi Yayını, 2002), 452.
[203] Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 4/1, (2002): 106.
[204] Yener Ünver, "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi", Journal of İstanbul University Law Faculty 59/1-2 (2011), 79.
[205] Yetim, "Mücadele Yöntemleri", 81.
[206] Akarslan, *Bilişim Suçları*, 36.
[207] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1025.; Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 32.
[208] Ünver, "İnternet Açısından", 79.; Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 32.; Yılmaz Yazıcıoğlu, "Bilgisayar Ağları", 452.
[209] Özbek, "İnternet Kullanımında", 107.
[210] Özbek, "İnternet Kullanımında", 107.
[211] Akbulut, "*Bilişim Alanında Suçlar*", 59.

ifadenin de bu suçları ifade etmekte yetersiz kaldığı görülmektedir[212]. Bu konuda başka bir eleştiri ise bilgisayar bu suçların işlenmesinde bir araç konumunda olduğundan[213] ve tek başına suç işleyemeyeceğinden dolayı, bu şekilde adlandırmanın hatalı olduğu ve nasıl bıçakla işlenen suçlar "bıçak suçu" olarak adlandırılmıyorsa, bilgisayar yoluyla işlenen suçların da "bilgisayar suçu" olarak adlandırılmasının isabetsiz olacağı yönündedir[214].

"Siber suç" yani sanal suç kavramı ise, bu suçların gerçeklik dışı olduğu algısı oluşturduğundan dolayı yeterli görülmemektedir[215]. Sonuç olarak işlenen suçlar tamamen gerçek suçlardır ve çoğu zaman ağlar aracılığıyla gerçekleştirilmesi bu suçları gerçeklikten uzak kılmamaktadır[216]. Başka bir görüşe göre ise bilişim suçları siber suçları da kapsayan daha geniş bir kavramdır[217].

"Elektronik suç" ifadesi ise bilişim sistemleri dışında diğer elektronik cihazların da olması ve bilişim suçlarının bu cihazların hepsini kapsayan suçlar olmamaları dolayısıyla uygun görülmeyen bir adlandırma olduğundan eleştirilmektedir[218].

"Bilgisayarlara karşı işlenen suç" ve "bilgisayar aracılığıyla işlenen suç" kavramları ise yeni suç işleme metotlarına uyum sağlamamaları noktasında ve bu tür suçlar hem bilgisayara hem de bilgisayarlara karşı diğer bilgisayarlar aracılığıyla işlenebildiğinden (yani bilgisayar bu suçlarda araç ve amaç konumunda bulunabileceğinden), tek yönlü bir ifade içermeleri yönüyle eleştirilmektedir[219]. Kaldı ki, bu suçların işlenebilmesi için bilgisayarların şart olmadığını herhangi bir bilişim sistemi aracılığıyla da işlenebileceğini daha önce belirtmiştik.

"Siber suçlar" ifadesinin her ne kadar bu suçları tanımlamada yaygın olarak kullanıldığı görülse de, "Bilişim Suçları" adlandırmasının hem mevzuatta hem öğretide hem de yargı bazında genel olarak kabul görmüş bir ifade olduğu ve bu konuda uzlaşı birliğine

[212] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1025.
[213] Ayhan Önder, *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar*, (İstanbul: Filiz Kitabevi, 1994), 504.
[214]Dursun, "Bilgisayar İle İlgili Suçlar", 339.
[215]Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1025.; Ünver, "İnternet Açısından", 79.
[216] Yılmaz Yazıcıoğlu, "Bilgisayar Ağları", 452.
[217] Yenidünya ve Değirmenci, *Mukayeseli Hukukta*,33.
[218] Akbulut, *Bilişim Alanında Suçlar*, 59.
[219] Dülger, *İnternet İletişim Hukuku*, 79.

varıldığı görülmektedir[220]. Gerçek manada bu alanın tamamını kapsar nitelikte açıklayıcı bir terim bulunmayıp, belirtilen tüm terimler birbiri alternatifi olarak kullanılsa da[221]; hangi terimle belirtildiği fark etmeksizin, bu suçların işleniş yeri bilgisayar ile yan teknolojilerinin birbirine bağlanmalarıyla oluşturdukları sanal alan ve çalıştıkları network sistemidir[222].

1.5.3. Bilişim Suçlarının İşleniş Şekilleri ve Bu Suçların İşlenmesinde Kullanılan Yöntemler

Bilişim suçlarının işlenmesinde öncelikle bir bilişim ortamının bulunması şart olup, bu bilişim ortamının temel elemanları bilgisayar ve benzeri cihazlar, veri iletişiminin gerçekleşebilmesi için bir iletişim ortamı ve cihazın çalışması için gerekli olan enerjiden oluşmaktadır[223]. Gerekli bilişim ortamının sağlanmasıyla birlikte, bilişim suçlarının dünyanın herhangi bir yerinde bulunan fail tarafından dünyanın herhangi bir yerinde bulunan mağdura karşı işlenebilmesi mümkün hale gelmektedir. Böylece fiili gerçekleştiren fail ile suçun mağdurunun farklı ülkelerden olmasına imkan tanıyan bu durum bilişim suçlarının işlenmesi, soruşturulması ve kovuşturulması açısından bilişim suçlarını klasik diğer suç tiplerinden ayıran en önemli can alıcı noktalarından birini oluşturmaktadır.

Bilişim suçlarını diğer klasik suç tiplerinden ayıran oldukça önemli özelliklerinden bir diğeri ise, bu suçların işlenmesinde kullanılan yöntemlerin karmaşıklığı ve çeşitliliğidir. Bunun temel sebebi de bu suçların işlenmesinin genellikle teknik bilgi gerektirmesi ve teknoloji ile bilişim suçlarının işleniş yöntemlerinin paralel bir biçimde gelişme göstermesiyle beraber, suçta kullanılan yöntemlerin her geçen gün farklılaşarak, takip edilmesinin öngörülemez bir yol izlemesidir.

Bilişim sistemleri kullanılarak günümüzde birçok farklı suç işlenebilmektedir. Veri hırsızlığı, tahribi, elektronik sabotaj, dolandırıcılık emniyeti suiistimal, hırsızlık, sahtecilik ve hatta örneğin sistem üzerinden hasta kayıtlarını değiştirmek suretiyle adam

[220] Dülger, *İnternet İletişim Hukuku*, 80.
[221] Murat Volkan Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık İngiltere Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması". *Türkiye Adalet Akademisi Dergisi*, 31 (2017): 147.
[222] Gün, "Bilişim Suçları", 67.; Yetim, "Mücadele Yöntemleri", 81.
[223] Akarslan, Bilişim Suçları, 37.

öldürmeye kadar birçok suç işlenebilmektedir[224]. Günümüzde bilişim suçları genellikle internet aracılığıyla gerçekleştirilmekte olup, bu suçların internet yoluyla yaygın ve sık bir biçimde işlenmesinin temelinde internetin anonim yapısı ile internette merkezi bir otoritenin, yani yönetim ve denetim mekanizmasının bulunmayışı temel etken olarak görülmektedir[225]. Doktrinde bazı yazarların suç işlenmesini oldukça kolaylaştıran ve suçların takibini zorlaştıran bir yapıda bulunması sebebiyle interneti vahşi batıya benzetmek suretiyle karşılaşılan zorlukları ifade ettikleri görülmektedir[226].

Bilişim suçlarının kendine has özelliklerinin yanında bu suçların faillerinin genel profillerinin yaptırımlardan etkilenme oranının düşük olması, caydırıcılıktan diğer klasik suç faillerine nazaran daha az etkilenmeleri bilişim suçlarının artmasında etken rol oynamaktadır. Faillerin genel profillerinde kendilerini işin uzmanı olarak görmeleri, kendilerini suçla mücadele eden görevlilerden daha becerikli ve üstün görmeleri, yakalanma risklerinin diğer suçlara göre daha düşük olması, yaş ortalamasının düşük olması, genellikle erkek olmaları ve sosyoekonomik durumlarının genelde düşük olmaması gibi özellikler görülmekte olup tüm bu özellikler caydırıcılıktan oldukça az etkilenmelerinde etken olmaktadır[227]. Bilişim suçlarına ve faillerine ilişkin özelliklerin karmaşık ve yenilikçi suç işleme yöntemleriyle de birleşmesiyle birlikte hem bu suçların soruşturma ve kovuşturmasında zorluklar ortaya çıkmakta hem de suç işleme oranlarının her geçen gün artmasına zemin hazırlamaktadır.

Bu suçların işlenmesinde her geçen gün farklı yöntemler geliştiriliyor olsa da günümüzde, temelde çok sık kullanılan, belli başlı suç işleme yöntemleri göze çarpmaktadır. Aşağıda yakın geçmişte yaygın olarak kullanılmış ve halen daha kullanılmakta olan belli başlı saldırı yöntemlerine yer verilecektir. Bunların bir kısmı eskisi kadar etkili görülmese de halen daha popüler bir şekilde kullanılmaya devam eden yöntemlerdir.

1.5.3.1. DoS-DDoS Saldırıları (Denial of Service – Distributed Denial of Services)

[224] Eker, "Eski TCK Bağlamında", 106.
[225] Eker, "Eski TCK Bağlamında", 106.
[226] Cahit Aliusta ve Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4/2 (2018), 35.
[227] Yılmaz ve Güllüpınar, "Kriminolojik Açıdan", 5381.

Türkçe ifadesiyle "Dağıtılmış ağ saldırıları" veya "Dağıtılmış hizmet saldırıları" olarak ifade edilebilen[228] DoS, bir sisteme yapılan düzenli ve sürekli saldırılarla sistemin çalışamaz hale getirilmesini sağlayan ve şahsen yapılan bir saldırı çeşidiyken, DDoS aynı saldırının önceden programlanmış birden fazla makine aracılığıyla yapılmasını ifade eder[229]. Dos saldırısında asıl hedef web uygulamaları değil de sunucular olup[230] tek kaynaktan tek bir hedefe yönelik olarak gönderilen veri paketleri, sunucunun cevap veremeyeceği nitelikte yoğun bir şekilde sunucuya gönderilerek, sistem kaynaklarını tüketir[231]. DDosda ise saldırganın bulunduğu sistem kontrol altına aldığı ağdaki diğer sistemleri kullanarak zombi bilgisayar ağı oluşturur ve bu ağı kullanmak suretiyle kendini de gizleyerek hedefine çoklu ataklar yapar[232]. Temelde bu saldırı çeşitleri ağ kaynaklarında eş zamanlı yapılabilecek işlemlerin ve sunucuyu ağa bağlayan bant kapasitesinin sınırlı olmasından faydalanarak sistemin çökmesini ve talep edilen hizmetin reddini sağlamaktadır[233]. Bu şekilde bir saldırı ile fail, örneğin bir şirkete veya bankaya ait bir web sitesini kullanılamaz hale getirmekte ve bunların itibarını hedef alarak, söz konusu firmaya zarar vermeye yahut fidye talebinde bulunarak maddi çıkar elde etmeye çalışmaktadır. Son zamanlarda bu saldırılara yönelik etkili savunma yöntemleri geliştirilmiş olsa da halen popüler olarak tercih edilen yöntemlerden birisidir[234].

1.5.3.2. Yemleme Saldırıları (Phishing)

İngilizcede "password harvesting" ve "fishing" kelimelerinin birleştirilmesiyle oluşturulmuş olup, Türkçede oltalama ve yemleme şeklinde ifade edilen bu yöntemde[235], kişiye dışarıdan bakıldığında güvenilir görünecek şekilde hazırlanmış sahte web siteleri veya mailler aracılığıyla, kişilerin gizli bilgilerinin elde edilmesi

[228] "DDoS Saldırısı Nedir?", (E. T. 15.01.2025), https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks
[229] Dülger, *İnternet İletişim Hukuku*, 123.
[230] Hamza Elbahadır, *Hacking Interface*, (İstanbul: Kodlab Yayıncılık, 2020), 117.
[231] M. Zekeriya Gündüz, "Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti", (Yüksek Lisans Tezi, Fırat Üniversitesi, 2013), 40.
[232] Gündüz, "Delil Tespiti", 41.
[233] "DDoS Saldırısı Nedir?"
[234] "En Sık Karşılaşılan 10 Siber Saldırı Yöntemi", (E. T. 15.01.2025), https://kron.com.tr/en-sik-karsilasilan-10-siber-saldiri-yontemi
[235] Aköz, "Mevzuat Önerileri", 33.

amaçlanır[236]. Bu noktada özellikle göze çarpan husus, hazırlanan sahte web sitelerinin bazılarının URL adreslerinin gerçeğine oldukça yakın olması ve dikkatli bakılmadığı sürece fark edilmemesinin oldukça olası olmasıdır. Bu yöntem genellikle şahısların şifre ve banka kartı bilgilerinin çalınmasına ve faillerin bu bilgilerle maddi çıkar sağlamasına hizmet etmektedir[237]. Bilişim suçlarının işlenmesinde en çok kullanılan yöntemlerden biri olan yemleme saldırıları özellikle internet bankacılığına yönelik saldırılarda uluslararası alanda yaygın bir şekilde kullanılmaktadır[238].

1.5.3.3. Kötü Amaçlı Yazılım (Malware)

Bilişim suçlarının işlenmesinde en yaygın kullanılan yöntemlerden biri de kötü amaçlı yazılımlar yoluyla sisteme yapılan saldırılardır. Malware, zararlı tüm yazılımların ortak genel adı olarak kullanılmakta olup, bu yazılımlar yoluyla bir bilişim sisteminin çalışamaz hale getirilmesi, uzaktan kontrolü, sistemde yer alan bilgilerin sızdırılması gibi birçok amaçla kullanılabilmektedir[239]. Üretim amacına göre değil de kullanım amacına ve özelliğine göre adlandırılan[240] bu zararlı yazılımlar; kimi zaman birlikte, kimi zaman tek başına kullanılmakta olup, birçoğu birbirleriyle iç içe geçmiş durumdadır. Bu yazılımlara; fidye yazılımları (Ransomwares), virüsler, Truva atları (Trojan Horses), botlar ve botnetler, rootkitler, casus yazılımlar (Spywares), reklam destekli yazılımlar (Adwares), mantık bombaları (Logic bombs), Tuzak kapanları (Trap Doors), tavşanlar (Rabbits), bukalemunlar (Chameleon) ve solucanlar (Worms) örnek verilebilir[241]. Bunları kısaca özetlemek gerekirse:

"Fidye yazılımları (Ransomware)" sistemde yer alan dosyaları kilitleyerek kullanıcının dosyalarına erişimine engel olur ve genellikle e-postalar aracılığıyla kimlik avı saldırısı düzenleyerek sisteme bulaşır[242]. Saldırgan sistemi kilitledikten sonra kullanıcıya ulaşarak şifrenin kaldırılması için fidye talebinde bulunur. Bu yöntemde göze çarpan husus, fidyenin genellikle büyük bir meblağ olmaması nedeniyle mağdurun

[236] Dülger, *İnternet İletişim Hukuku*, 123.
[237] "10 Siber Saldırı"
[238] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı , "Dijitalleşen Dünyada", 28.
[239] "10 Siber Saldırı"
[240] Akarslan, Bilişim Suçları, 90.
[241] "Malware Nedir? Çeşitleri Nelerdir?" (E. T. 15.01.2025) https://www.niobehosting.com/blog/malware-nedir/.
[242] "Malware Nedir?"

ödemeyi göze alması, saldırganın da ödeme gerçekleştikten sonra şifreyi göndererek güven oluşturması ve sonuç olarak mağdurun çoğunlukla suç duyurusunda bulunmamasıdır[243]. Fail bu yöntemde genellikle ifşa olmamak adına fidyenin kripto para birimleri ile anonim bir hesaba aktarılmasını talep etmektedir[244].

İlk örneğinin bir lise öğrencisi tarafından 1982'de üretildiği kabul edilen[245] **"Virüsler (Viruses)"** genellikle sabotaj amacıyla kullanılan[246], çoğu zaman mailler ve internet üzerinden indirilen programlar aracılığıyla yayılan, kendini çoğaltabilen, çoğalttığı kopyalarını bulunduğu sistemden başka sistemlere de bulaştırarak kendiliğinden yayılan ve veri karıştırma, program silme, sistem çalışmasını engelleme gibi etkilere yol açan zararlı yazılımlardır[247]. Bilişim uzmanlarınca virüslerin evriminde maddi çıkar sağlama amacıyla sanal suçlara yönelimin artmasının büyük bir etken olduğu vurgusu yapılarak binlerce virüs programının üretildiği belirtilmiştir[248]. Virüslerde göze çarpan husus; ilk etkileşimin kullanıcı tarafından farkında olmadan başlatılması ile devreye girmeleri, ancak devreye girdikten sonra kendi başlarına yayılım ve etki göstermeleridir[249]. En sık karşılaşılan virüs türü ".exe" uzantılı dosyalar yoluyla bulaştırılan virüsler olup bu tarz virüsler dosyanın çalıştırılması suretiyle sisteme bulaşarak yayılırlar[250]. En tehlikeli ve en bilindik zararlı yazılımlardan biridir.

Adını mitolojiden alan **"Truva atları (Trojan Horse)"** özellikle ücretsiz indirilen programların içerisine gizlenerek, programın indirildiği cihaza bulaşan ve gönderen kişinin sistemi arka planda ele geçirmesine hizmet eden kötü amaçlı yazılım türüdür[251]. Kullanıcının yüklediği asıl program hedeflediği şekilde çalışırken, arka planda failin komut vermesi veya yazılımın önceden girilen emirleri uygulayarak faile hizmet etmesi söz konusudur[252]. Truva atları sisteme girme, veri ele geçirme ve verilere zarar verme gibi birçok amaçla kullanılabildiğinden, özellikle devletlerarası casusluk eylemlerinde

[243] Dülger, *İnternet İletişim Hukuku*, 129.
[244] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı , "Dijitalleşen Dünyada", 30.
[245] Pallı, "Hukukta Bilişim Suçları", 58.
[246] Akbulut, *Bilişim Alanında Suçlar,* 78.
[247] Mert Asker Yüksektepe, *Bilişim Suçları ve Soruşturma Usulü*, (İstanbul: Platon Plus Yayıncılık, 2022), 66.
[248] Akarslan, Bilişim Suçları, 91.
[249] Akbulut, *Bilişim Alanında Suçlar*, 77.
[250] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, "Dijitalleşen Dünyada", 29.
[251] Dülger, *İnternet İletişim Hukuku,* 110.; Elbahadır, *Hacking Interface,* 110.
[252] Akbulut, *Bilişim Alanında Suçlar*, 79.

sıkça kullanılmaktadır[253]. Virüslerden en önemli farkı, virüsler gibi kendini kopyalama ve tüm sisteme yayılma özelliklerinin bulunmamasıdır[254]. Yayılması için kullanıcının Truva atının saklandığı dosyayı indirerek veya bulunduğu mail eklentisini açarak yürütmeyi başlatması gerekir[255]. Bilişim suçları işlenirken sıklıkla uygulanan yöntemlerden birisidir.

"Botlar ve Botnetler" genellikle diğer zararlı yazılımlar aracılığıyla ele geçirilen sistemlerin topluca uzaktan yönetilerek başka bir saldırı düzenlemek amacıyla kullanılmasıdır[256]. "Robot" ve "net" kelimelerinin birleştirilmesi ile oluşturulan "Botnet" kavramı, ele geçirilen ve saldırganların kurban olarak adlandırdıkları zombi (bot) cihazları kullanarak oluşturulan geniş bir bot ağıdır[257]. Bu yöntemle hem bot cihaza karşı hem de bot cihaz vasıtasıyla suç işlenebilmektedir[258]. Botnetler özellikle DDoS saldırılarında kullanılmakla birlikte bir web sitesinin tıklanma oranını artırmak ve çıkar elde etmek amacıyla da kullanılmaktadır[259]. Örnek bir olay 2016'da gerçekleşmiş, nesnelerin interneti (IoT) sistemlerini hedef alarak bunları bir botnete dahil etme hedefi olan ve Mirai adı verilen kötü amaçlı bir yazılım, ABD'de büyük çaplı bir internet erişimi sıkıntısı ortaya çıkarmıştır[260].

"Kök Kullanıcı Takımı[261] (Rootkits)" ortadan kaldırılması ve tespiti oldukça zor olan, bir sisteme uzaktan erişim veya sistemi kontrol etmek amacına hizmet eden tehlikeli bir kötü amaçlı yazılımdır[262]. Rootkitleri diğer zararlı yazılımlardan ayıran en önemli özelliği tamamen gizlilik üzerine oluşturulmalarıdır[263]. İlk başta Unix İşletimi Sistemi için üretilmiş olmakla beraber sonradan diğer sistemlerde de kullanılmaya başlanmıştır[264]. Yönetici düzeyinde kontrole imkân veren rootkitler genellikle yazılım

[253] Dülger, *İnternet İletişim Hukuku*, 111.
[254] Akbulut, *Bilişim Alanında Suçlar*, 79.
[255] Pallı, "Hukukta Bilişim Suçları", 54.
[256] "Malware Nedir?"
[257] Dülger, *İnternet İletişim Hukuku*, 124.
[258] Aköz, "Mevzuat Önerileri", 39.
[259] Dülger, *İnternet İletişim Hukuku*, 125.
[260] "Farklı kötü amaçlı yazılım türleri nelerdir?", (E. T. 15.01.2025), https://www.kaspersky.com.tr/resource-center/threats/types-of-malware.
[261] Akarslan, Bilişim Suçları, 96.
[262] "Malware Nedir?"
[263] Elbahadır, *Hacking Interface*, 238.
[264] Akarslan, Bilişim Suçları, 96.; Elbahadır, *Hacking Interface*, 237.

ve işletim sistemini etkilemekle birlikte, bazıları donanımı da etkileyebilmektedir[265]. Günümüzde ev aletleri gibi birçok nesne ağ bağlantısı kullanmaya başlamış olup nesnelerin interneti geliştikçe, tüm bu cihazlarda bu zararlı yazılımın hedefi olabilecek[266], örneğin akıllı robot süpürgeleri ele geçirilerek kişiler izlenebilecek ve konutun detayları ve mevcut durumu öğrenilerek hırsızlık suçu için kullanılması gündeme gelebilecektir.

"Casus Yazılımlar (Spywares)" adı üzerinde bilişim sisteminin içerisine sızan birer casusturlar ve failin sistem kullanıcısının hareketlerini izlemesini sağlarlar[267]. Casus yazılımlar virüsler gibi kendini çoğaltarak bir ağa veya diğer sistemlere yayılma gereksinimi duymaz, girdiği sistemi izleyerek bilgi edinmek ve hassas verileri ele geçirmek temel amacıdır[268].

"Reklam Destekli Yazılımlar (Adwares)" kullanıcının iznini almadan istemediği reklamlara maruz kalmasını sağlayan kötü amaçlı bir yazılım türüdür[269]. Özellikle kullanıcılara ilişkin istatiksel verileri pazarlama amacıyla ve reklam geliri sağlama amacıyla kullanılmaktadır[270].

"Mantık Bombaları (Logic Bombs)" koşullandırılmış bir zararlı yazılım türüdür. Tetiklenmeyi bekleyen mantık bombaları, bir zaman dilimi geçtikten sonra, belli bir tarihte veyahut belli hareketlerin belli bir seviyede tekrarlanması üzerine harekete geçmek üzerine tasarlanmıştır ve harekete geçtikten sonra yol açtığı hasar oldukça büyüktür[271]. Sistemi şaşırtmak, bozmak ya da felç etmek için programlanan ve belirlenmiş özel durum gerçekleşene kadar bir truva atı programı gibi davranan mantık bombaları bilgisayara sürekli olarak ya mantık dışı ya da yapılan işlemin aksine bilgiler göndermektedir[272]. Mantık Bombaları ilk olarak 1992'de bir General Dynamics çalışanının yaşamsal roket proje verilerini yok edebilecek bir mantık bombasını sisteme

[265]"Rootkit nedir", (E. T. 15.01.2025), https://www.kaspersky.com.tr/resource-center/definitions/what-is-rootkit.
[266]"Rootkit nedir".
[267] "Malware Nedir?"
[268] Akbulut, *Bilişim Alanında Suçlar*, 85.
[269] "Malware Nedir?"
[270] Akarslan, Bilişim Suçları, 95.
[271] "yazılım türleri nelerdir?".
[272] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, "Dijitalleşen Dünyada", 33.

sokmasıyla ortaya çıkmıştır[273]. Tarihte kişisel bilgisayarlara karşı yapılan ilk saldırı bu zararlı yazılımla gerçekleştirilmiş, ABD'de gerçekleşen olayda ücretsiz deneme paketi verilen kullanıcıların paketi denedikten sonra kullanmak istemeyip ücret ödemeyenlerinin önce sistemleri kilitlenmiş sonrasında ise verileri silinerek sistem kendisini yok etmiştir[274]. Bu zararlı yazılıma başka bir örnek de 1999'da Türkiye'de CIH isimli bir virüsün, üreticisi tarafından bir konferansta yararlı olarak gösterilip yerli yabancı katılımcılara dağıtılarak yayılması ve birçok bilişim sistemine zarar vererek büyük hasara yol açması gösterilebilir[275].

"Tuzak Kapanları (Trap Doors)" sistemin standart kimlik doğrulama aşamalarını atlamayı veya uzaktan erişimi sağlayan, sistem kurulurken açık unutulan veyahut fail tarafından sisteme sızıldıktan sonra kolay bir geçiş noktası olarak bırakılan ve back doors (arka kapı) olarak adlandırılan[276] zayıf noktalara yerleştirilen zararlı yazılımlardır. Bu kapılar genellikle işletim veya çok işlevli kullanıcı sistemlerini hazırlayan programcıların bunları meydana getirirken, sistem tamamlanana kadarki süreçte, ileride ortaya çıkabilecek durumlara karşı sisteme bıraktıkları, ancak ya hata sonucu veya ileride kullanılmak amacıyla orada bıraktıkları çeşitli giriş yollarına denmektedir[277]. 2018'de gerçekleşen örnek bir olayda Türkiye, Rusya ve Ukrayna'da back door içeren bir program nedeniyle çok sayıda bilgisayara zararlı yazılım bulaşmıştır[278].

"Tavşanlar (Rabbits)" çok hızlı çoğalabilen, girdiği sistemin işlemcisine sürekli anlamsız komutlar yükleyerek sistemin normal çalışmasının önüne geçen ve bir süre sonra da çalışmaz hale getiren, çoğunlukla çok kullanıcılı sistemleri hedef alan bir zararlı yazılım çeşididir[279]. Sistemin işlem kabiliyetini kısıtlar ve sistemi boş yere doldurur[280]. Girdikleri sistemi ve ağ trafiğini bozma yetkinliğine sahip olan rabbitler, başka programlara yayılım göstermezler, yalnızca bulundukları sistemi etkilerler[281]. Virüslerden en belirgin farkı asalak özellikte olmayıp kendi kendilerine

[273] Pallı, "Hukukta Bilişim Suçları", 56.
[274] Akbulut, *Bilişim Alanında Suçlar*, 83.
[275] Dülger, *İnternet İletişim Hukuku*, 118.; Akbulut, *Bilişim Alanında Suçlar*, 83.
[276] Akbulut, *Bilişim Alanında Suçlar*, 87.
[277] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, "Dijitalleşen Dünyada", 34.
[278] Aköz, Mevzuat Önerileri, 35.; STM ThinkTech, "Siber Tehdit Durum Raporu (Ocak-Mart 2018)", https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2018, 16.
[279] Dülger, *İnternet İletişim Hukuku*, 116.
[280] Aköz, Mevzuat Önerileri, 40.
[281] Akbulut, *Bilişim Alanında Suçlar*, 82.

yetebilmeleridir[282]. Örnek bir olayda işten çıkarılan bir programcı şirketin sistemine Sarmaşık adında bir rabbit yükleyerek 20 gün sonra sistemin sarmaşığın kopyalarıyla dolup taşmasına ve hiçbir işlemi yürütemez hale gelerek hizmet verememesine neden olmuştur[283].

"Bukalemunlar (Chameleons)" taklitçi bir zararlı yazılım çeşididir. Mevzuata uyumlu yazılımların her hareketini ve ağ giriş iletilerini birebir taklit eder[284]. Çoklu ağ sistemlerinde etkindirler[285]. Öncelikle zararsız bir yazılım görünümü çizen ve kendilerini oldukça iyi bir şekilde gizleyen bukalemunlar, sisteme girdikten sonra zarar verici faaliyetlerine başlayarak, sistemdeki kullanıcı verilerini ve şifreleri kaydeder ve geçici bakım uyarısı vererek, sistem kapandıktan sonra failin eylemlerini gerçekleştirmesine izin verir[286]. Özellikle bankaların bilişim sistemlerine yönelik gerçekleştirilen hukuka aykırı yarar sağlama suçlarında etkin olarak kullanılan bir yöntemdir[287].

Birçok farklı türü bulunan **"Solucanlar (Worms)"** virüslere benzerlik göstermekle beraber virüslerdeki gibi başka bir programın arkasına gizlenme veya kullanıcı tarafından etkinleştirilme ihtiyacı duymayan zararlı yazılımlardır[288]. Herhangi bir yazılımsal ya da donanımsal zarara sebep olmaksızın sistemden sisteme dolaşabilmektedirler[289]. Çok sık karşılaşılan kötü amaçlı yazılımlardan biri olup sistemin açıklarından faydalanarak ağa girdikten sonra herhangi bir kullanıcının eylemine ihtiyaç duymadan kendini çoğaltarak ağ üzerinde yer alan diğer sistemlere de yayılabilir ve veri çalma, fidye amaçlı şifreleme, botnet oluşturma, veri yok etme gibi birçok fiilde kullanılabilir[290]. Yayılmak için ağları kullanması sebebiyle de çoğu zaman ağ solucanları olarak da adlandırılır[291]. Sistemden sisteme atlayarak gerekli oldukça üreyen ve sistemde oldukça gizli bir şekilde dolaşan solucanlar, gerektiğinde

[282] Pallı, "Hukukta Bilişim Suçları", 59. Emin Doğan Aydın, *Bilişim Suçları ve Hukukuna Giriş*, (Ankara: Doruk Yayınları, 1992), 53.
[283] Aköz, Mevzuat Önerileri, 40.
[284] Akbulut, *Bilişim Alanında Suçlar*, 82.; Aydın, *Bilişim Suçları,* 51.
[285] Yüksektepe, *Soruşturma Usulü*, 62.
[286] Dülger, *İnternet İletişim Hukuku*, 117.; Akbulut, *Bilişim Alanında Suçlar*, 82.; Aydın, *Bilişim Suçları*, 51.
[287] BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı , "Dijitalleşen Dünyada", 34.
[288] Akbulut, *Bilişim Alanında Suçlar*, 80.
[289] Pallı, "Hukukta Bilişim Suçları", 59.; Aydın, *Bilişim Suçları,* 53.
[290] "Yazılım Türleri Nelerdir?".
[291] Akarslan, Bilişim suçları, 92.

hafızasında yer alan yaygın şifreleri de tek tek denemek suretiyle sistem şifrelerini kırar ve hedefine girmeyi başarır[292]. Gerçekleşen bir olayda 2003 yılında ortaya çıkan ve standartlardan farklı bir yol izleyerek yeni IP adresleri oluşturup bu IP'ler aracılığıyla korunması olmayan sistemlere erişen SQL Slammer adlı bir solucan 75.000'den fazla bilgisayar aracılığıyla birçok büyük web sitesine DDoS saldırıları gerçekleştirmiştir[293].

Bahsettiğimiz tüm bu zararlı yazılım türleri dışında dialers (telefon çeviriciler), key logger (tuş kaydediciler), screen logger (ekran kaydediciler) ve scareware gibi bahsetmediğimiz daha birçok farklı zararlı yazılım türü de bulunmaktadır.

1.5.3.4. Ortadaki Adam Saldırısı (Man In The Middle Attack)

Yetkisiz erişim yoluyla ağ cihazları ile kurban bilgisayarlar arasındaki iletişimi kesintiye uğratıp bu sırada veri paketlerini anında yakalayıp işleyerek verilerin gizli bir şekilde ele geçirilmesine olanak sağlayan bir saldırı türüdür, bu yöntem kısaca ağdaki paketleri yakalayıp manipüle etmektedir[294]. Kablosuz ağ bağlantılarında kullanılan[295] ve bir tür gizli dinleme olan bu saldırı sırasında mağdur hiçbir şey olmamış gibi internete bağlanmaya devam eder ancak bilgisayarla bağlantı kurduğu tüm siteler fail için artık görünür durumdadır[296]. Hedef genellikle çevrimiçi bankacılık ve e-ticaret web sitelerine ait bilgiler olsa da, kimlik hırsızlığı (taklit) ve kötü amaçlı web sitelerine yönlendirme gibi hedefler de söz konusu olabilmektedir[297]. Açık Wi-Fi kullanımı ve IoT cihazlarının savunmasızlığı son yıllarda bu saldırıların artmasına neden olmuştur[298].

1.5.3.5. Yapılandırılmış Sorgu Dili Aşılaması (SQL İnjection)

Web sayfaları ve web uygulamalarının güvenliğini aşarak yapılandırılmış sorgu dili anlamına gelen ve veri tabanları için komut ve kontrol dili olan SQL veri tabanının içeriğini ele geçirmeyi hedef alan bir saldırı türüdür[299]. Web uygulamalarının

---

[292] Akbulut, *Bilişim Alanında Suçlar*, 80.
[293] "Yazılım Türleri Nelerdir?".
[294] Ahmet Efe, Gizem Kalkancı, Mehmet Donk, Serhat Cihangir ve Ziya Uysal, "A Hidden Hazard: Man-In-The-Middle Attack in Networks", *Computer Science*, 4/2 (2019): 99.
[295] Yüksektepe, *Soruşturma Usulü*, 51.
[296] Efe vd., "A Hidden Hazard", 99.
[297] Efe, vd., "A Hidden Hazard", 99.
[298] "Ortadaki Adam (MitM) Saldırısı Nedir?", (E. T. 15.01.2025), https://www.turhost.com/blog/ortadaki-adam-mitm-saldirisi-nedir/#serp.
[299] "SQL Injection Nedir?", (E. T. 15.01.2025), https://www.turhost.com/blog/sql-injection-nedir/#serp.

kodlanması sürecinde dikkatsizlik sonucu yapılan hatalar ve gerekli önlemlerin alınmamış olması bu web uygulamalarına yönelik komut saldırılarının gerçekleştirilebilmesine zemin hazırlamaktadır[300]. Saldırgan güvenliği aştıktan sonra özel hazırlanmış bir SQL komutunu bir saldırı olarak çalıştırır ve karşılığında veri tabanı hassas bilgilere erişim sağlayan bir yanıt oluşturarak saldırgana iletir[301]. Veritabanı kullanan web sitelerinin ve sunucuların yaygın olması nedeniyle oldukça sık kullanılan bu yöntemle fail; hassas verileri çalma, verileri değiştirme, sisteme yönetici olarak erişim sağlama gibi birçok fiili gerçekleştirebilmektedir[302]. Bu saldırı yöntemiyle gerçekleştirilen örnek bir olay 2009'da gerçekleşmiş; 7-Eleven perakende zinciri başta olmak üzere birçok kurumsal şirketin sistemlerine yapılan saldırıda 130 milyon kredi kartı numarası failler tarafından ele geçirilmiştir[303].

1.5.3.6. Gizli Dinleme (Eavesdropping Attack)

Genellikle kötü amaçlı yazılımlar yoluyla ağ trafiğini ya da iletişim kanallarını takip ederek hassas verileri ele geçirme amacı güden bu saldırılar, iletişimi manipüle etme ve kontrol etme gibi özellikleri bulunan MitM saldırısından yalnızca izleme fiilini gerçekleştirmeleri yönüyle ayrılırlar[304]. Bu tarz saldırılar bilgisayar ekranının elektromanyetik dalgaları yakalanarak ekran görüntüsü elde edilmek suretiyle de gerçekleştirilebilmektedir[305].

1.5.3.7. Parola Kırma Saldırıları (Passwords Attack)

Bir bilişim sisteminde yer alan verilerin şifrelerini çözmek için yapılan saldırılardır[306]. Parola kırma saldırıları birçok farklı tarzda gerçekleştirilebilmektedir. "Brute Force Attacks" (Kaba Kuvvet Saldırısı) olarak bilinen yöntemde olabilecek tüm kombinasyonlar kullanılarak şifre kırılmaya çalışılırken, "Dictionary Attacks" (Sözlük

[300] Gündüz, "Delil Tespiti", 48.
[301] "SQL Injection Nedir? Nasıl Tespit Edilir? Nasıl Engellenir?", (E. T. 15.01.2025), https://www.niobehosting.com/blog/sql-injection/.
[302] "SQL aşılama nedir?", (E. T. 15.01.2025), https://www.kaspersky.com.tr/resource-center/definitions/sql-injection.
[303] "SQL Injection Nedir?".
[304] Eavesdropping Attack, (E. T. 15.01.2025), https://cahitcengizhan.com/eavesdropping-attack/#:~:text=Eavesdropping%20attack%20(ya%20da%20dinleme,hassas%20bilgileri%20elde%20etmeyi%20ama%C3%A7lar.
[305] Yüksektepe, *Soruşturma Usulü*, 61.
[306] Dülger, *İnternet İletişim Hukuku*, 123.

Saldırısı) yalnızca başarılı olma olasılığının yüksek olduğu kombinasyonları dener[307]. Bunlar dışında internette en çok kullanılan şifrelerin bir listesi kullanılarak parola kırma yöntemi olan Password Spraying gibi yöntemler olduğu gibi; oltalama saldırısı gibi diğer saldırı yöntemleri veyahut kötü amaçlı yazılımlar kullanılarak da parolaların ele geçirilmesi mümkündür[308].

Tüm bu yer verdiğimiz yöntemler dışında bilişim suçlarının işlenmesinde cryptojacking, zero day exploit, supply chain attack[309], salam tekniği, çöpe dalma, piggybacking, masquerading[310] gibi daha birçok suç işleme yöntemi bulunmakla birlikte, zamanla bilişim suçu faillerinin yöntemlerini geliştirdiği ve teknolojinin gelişimiyle birlikte bazı yöntemlerin kullanımının ve kullanım alanının oldukça genişlediği görülmektedir. Örneğin son zamanlarda sanal gerçeklik (VR) teknolojisi açısından "Inception Saldırıları" adı verilen yeni bir saldırı türünün güvenlik açığı oluşturduğu ve bu yolla kullanıcı verilerinin ele geçirilebileceği belirtilmekte, ayrıca siber casusluk ve propaganda için kullanılabileceği ifade edilmektedir[311]. Yine son zamanlarda "Web Shell" adı verilen kötü amaçlı komut dosyaları kullanılarak yapılan saldırıların yaygınlaştığı ve özellikle sağlık sektörünü hedef alan saldırıların yapıldığı görülmüştür[312]. Bilişim sistemlerinin sağlık sektöründe olduğu gibi diğer birçok sektörde kullanımının yaygınlaşması ve buna yönelik korumanın aynı hızda sağlanamıyor oluşu özellikle bilişim suçu faillerini cezbetmekte ve bu konudaki tehlikenin artmasına neden olmaktadır. Tüm bunlarla birlikte bilişim sistemlerinin güvenliğinin nükleer santraller nezdinde de tesisin emniyeti ve güvenli çalışması için oldukça önemli olduğu, siber terörizm kapsamında nükleer terörizm kavramından bahsedildiği, nükleer reaktörlere karşı fiziksel zarar verebilen siber saldırıların mümkün olduğu ve geçmişte Dos saldırıları, virüs, solucan ya da hack şeklinde tek boyutlu saldırılarken; son zamanlarda slammer worm, stuxnet siber saldırısı gibi çeşitli saldırı

[307]Maşite Danışman, Password Attacks, (E. T. 15.01.2025), https://www.siberguvenlik.web.tr/password-attacks-sifre-saldirilari/.
[308] Danışman, Password Attacks.
[309] "10 Siber Saldırı".
[310] Bkz: Dülger, *İnternet İletişim Hukuku*, 109 vd.
[311]STM ThinkTech, "Siber Tehdit Durum Raporu (Ocak-Mart 2024)", https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2024, 7.
[312]"En Yaygın Siber Saldırı Türü: Web Shell En Çok Hedef Alınan Sektör: Sağlık", (E. T. 15.01.2025), https://www.cybermagonline.com/en-yaygin-siber-saldiri-turu-web-shell-en-cok-hedef-alinan-sektor-saglik.

yöntemleriyle saldırıların çok boyutlu bir hale bürünerek teknolojiyle orantılı bir biçimde tehlikelerin katlandığı ifade edilmektedir[313].

1.5.4. Dünyada Bilişim Suçları

Bilgisayarların ortaya çıkışı ve teknolojinin gelişimiyle beraber bilişim alanının suçta kullanılmaya başlaması uluslararası çerçevede bu konuda özel bir düzenleme yapılmasının gerekip gerekmediği konusunda tartışmalara yol açmış, kanuni düzenlemeyi gereklilik olarak görenler suç dünyasında nitel ve nicel değişikliklere yol açan bilgisayarlar ile işlenen fiillerin genel suçlar içerisinde değerlendirilmesinin kanunilik ilkesi ve kıyas yasağına aykırılık teşkil edeceğini savunmuş, düzenlemeyi gereksiz bulanlar ise bilgisayarların bu konuda bir yenilik getirmediğini, düzenlemenin teknolojik gelişmelerin önüne geçeceğini öne sürmüştür[314]. Bu tartışmanın sonucunda düzenlemeyi gerekli gören görüş ağır basmış ve bir yandan bu konuda uluslararası sözleşmeler hazırlanırken bir yandan da birçok ülkede ulusal düzenlemeler oluşturulup yürürlüğe sokulmuştur. Ulusal düzenlemeler konusunda ülkeler arasında farklılıklar gözlenmiş, ABD, İngiltere gibi kimi ülkeler özel kanunlar yapma yolunu tercih ederken, İtalya, Almanya gibi kimi ülkeler mevcut hükümlerde değişiklik ve eklemeler yaparak bilişim suçlarını kapsar şekilde genişletme yoluna gitmiş, Fransa, Portekiz gibi bazı ülkeler ise ceza kanunlarına ayrı başlıklar açarak mevcut kanunlara yeni hükümler eklemiştir[315].

Bilişim suçlarına dair düzenlemeler ülke iç hukukları bazında incelendiğinde İngiltere ve ABD'nin yer aldığı Anglo-Sakson hukuk ve diğer birçok ülkenin yer aldığı Kıta Avrupası sistemi olmak üzere genel olarak iki tür sisteme göre normlar konulduğu görülmektedir[316]. Yönetim şekillerine göreyse; üniter yönetimlerde tüm ülkeyi kapsayan kanunlar düzenlenirken, ABD gibi federal devletlerde kendine özgü federal kanunlar düzenlendiği görülmektedir[317].

---

[313] Detaylı bilgi için bkz: Cihad Furkan Eliaçık, *Uluslararası Hukuk Bağlamında Nükleer Santrallerin Siber Güvenliği*, (Ankara: Seçkin Yayınları, 2018), 129-131.
[314] Akbulut, *Bilişim Alanında Suçlar*, 89.
[315] Akbulut, *Bilişim Alanında Suçlar*, 90.
[316] Ermeydan, *Türk Ceza Kanunu'nda Bilişim Suçları*, *Türk Ceza Kanunu'nda Bilişim Suçları*, (Ankara: Seçkin Yayınları, 2023), 80.
[317] Ermeydan, *Bilişim Suçları*, 80.

1.5.4.1. ABD

Bilgisayar ve internetin icadında merkez konumunda bulunan Amerika Birleşik Devletleri'nde bilişim suçlarının ortaya çıkışı ve yaygınlaşması da hızlı bir biçimde gelişim göstermiş ve işlenen suçlarla mücadele noktasında da ilk adımlar bu devlette atılmıştır. Günümüzde de görüldüğü üzere, ABD dünya çapında faaliyet gösteren Microsoft, Google gibi dev bilişim şirketlerine sahip olup, bu şirketler ülke ekonomisinde büyük katkıya sahiptirler ve bu sebeple de bilişim alanının korunması ülke ekonomisi açısından önem arz etmektedir[318]. Bu alana verdiği önem ülkede bu alanda çalışmalar yapan CIA(Merkezi İstihbarat Teşkilatı), IC3 (İnternet Suç Şikayet Merkezi) NW3C (Ulusal Beyaz Yaka Merkezi) gibi birçok kurum ve kuruluşun mevcudiyetinden de anlaşılabilmektedir[319]. ABD'nin bu konuya verdiği önemin bir diğer göstergesi de Avrupa Konseyi üyesi olmadığı halde Avrupa Konseyi Siber Suç Sözleşmesi'ne imza atmış olmasıdır[320].

ABD'nin federal bir devlet olması dolayısıyla bünyesindeki eyaletler ile federal devlette farklı çeşitli düzenlemelerin mevcut olduğu görülmektedir[321]. Federal düzeyde yapılan düzenlemelerden en temeli[322] güvenlikli bir bilgisayara yetki ve izin olmaksızın erişimi yasaklayan ve 1984'te çıkarılan Bilgisayar Sahtekârlığı ve Bilgisayarın Kötüye Kullanılması Kanunu (Computer Fraud and Abuse Act) olup bu kanunun süreç içerisinde yeterli görülmemesi nedeniyle yıllar içerisinde üzerinde birçok değişiklik yapılmıştır[323]. Özellikle 1986'da yapılan değişiklikle ulusal savunma ve yurtdışı ilişkilerle ilgili veya herhangi gizlilik içeren bir bilginin ABD'de çıkarılan idari düzenlemelere aykırı olarak devlet aleyhine veya üçüncü bir devlet yararına ifşası suç olarak düzenlenmiştir[324]. Bunun dışında müstehcen yayın yasağı getiren ve bilişim suçlarıyla mücadelede tarihsel açıdan oldukça önemli görülen İletişim Ahlakı Kanunu (Communications Decency Act – CDA) çıkarılmış ancak getirilen hükümler antidemokratik oldukları gerekçesiyle Anayasa'ya aykırı görülerek iptal edilmiştir[325].

[318] Dülger, *İnternet İletişim Hukuku*, 224.
[319] Özüdoğru, "Mücadele Yöntemleri", 71.
[320] Dülger, *İnternet İletişim Hukuku*, 225.
[321] Tunç Demircan, *Bilişim Alanında Suçlar*, (İstanbul: Legal Yayıncılık, 2016), 32.
[322] Dülger, *İnternet İletişim Hukuku*, 225.
[323] Özüdoğru, "Mücadele Yöntemleri", 73.
[324] Demircan, *Bilişim Alanında Suçlar*, 32.
[325] Özüdoğru, "Mücadele Yöntemleri", 74.

Buna benzer olarak 1996 yılında çıkarılan diğer bir kanun da çocukların suiistimalini önlemek amacıyla düzenlenen Çocuk Pornografisinin Önlenmesi Kanunu (Child Pornography Prevention Act –CPPA) olup, özgürlükleri çok geniş bir biçimde kısıtladığı gerekçesiyle bazı hükümleri iptal edilmiştir[326]. Yine 1998'de çocukları müstehcen yayınlardan korumaya yönelik olarak Çocukların Online Yayınlardan Korunması Kanunu (Child Online Prevention Act – COPA) çıkarılmış, 2000'lerde ise kanun yerel mahkemece ve istinaf yolunda Anayasaya aykırı görülmüş[327] ancak temyiz incelemesinde aykırılık bulunmadığına karar verilmiştir[328]. Görüldüğü üzere ABD'de bu alanda çıkarılan birçok kanun hürriyetleri kısıtlayıcı olduğu ve antidemokratik nitelik taşıdığı gerekçeleriyle eleştirilerek iptalleri için yargı yoluna başvurulmuştur. Özellikle hürriyet sansürünü engellemek isteyen sivil toplum örgütlerinin bu kanunlara yönelik yapmış olduğu eylemler, iptal istemlerinde oldukça etkili olmuştur. Bununla beraber tüm bu iptal istemlerine rağmen ABD'de bu alanın korunmasına yönelik adımlar atılmaya devam edilmiş ve sayılan bu kanunlar dışında *elektronik haberleşmenin gizliliği, internette kumarın önlenmesi, kimlik hırsızlığı ve terörizmle mücadele*[329] gibi konularda da yine birçok düzenleme yapılarak bilişim alanında korumanın genişletilmesi ve suçun önlenmesi amaçlanmıştır. 2001 yılında yeni Terörizmle Mücadele Kanunu yürürlüğe sokularak, bazı güvenlik hizmeti veren bilişim sistemlerine ve bu sistemlerde bulunan verilere karşı saldırılar "sanal terörizm suçu" adı altında düzenlenerek yaptırıma bağlanmıştır[330]. Bununla birlikte ABD'de bilişim suçları ve bilişim yoluyla işlenen suçların ayrı ayrı ele alındığı ve farklı kanuni düzenlemeler oluşturulduğu görülmektedir[331].

ABD'de korumalı bir bilgisayara hukuka aykırı olarak erişim ve bilgisayar verilerinin tahrip edilmesi ve değiştirilmesi suç olarak düzenlenmiştir[332]. Ayrıca ABD Federal Ceza Kanunu m. 1030'da, hükümete zarar vermek ya da başka ülkeye yarar sağlamak saiki ile savunma ve dışişlerine tasnif edilmiş ve gizlilik kapsamında olan bilgiye izinsiz

[326] Dülger, *İnternet İletişim Hukuku*, 227.
[327] Özüdoğru, "Mücadele Yöntemleri", 75.
[328] Dülger, *İnternet İletişim Hukuku*, 228.
[329] Bkz: Dülger, *İnternet İletişim Hukuku*, 228-230.
[330] Gün, "Bilişim Suçları", 157.; Dülger, *İnternet İletişim Hukuku*, 229.
[331] Hüseyin Akarslan, "Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı", (Yüksek Lisans Tezi, T.C. Polis Akademisi, 2011), 112.
[332] Fatma Burcu Nacar, "Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları", (Yüksek Lisans Tezi, Atılım Üniversitesi, 2010), 40-42.

erişim, finansal bir kurumun finans kayıtlarına, tüketici bilgilerine ulaşmak ya da bunları kullanmak amacıyla bir bilgisayara hukuka aykırı girişin de yine suç olarak düzenlendiği görülmektedir[333].

1.5.4.2. Fransa

Fransa'da bilişim suçları ilk başta mal aleyhine işlenen hırsızlık, dolandırıcılık gibi suç tipleri içerisinde değerlendirilmiş, 1988'de ise kanuna bu suçlara mahsus düzenlemeler getirilmiştir[334]. İlerleyen süreçte de bilişim suçlarına özel bir kanun çıkarmak gerekli görülmemiş, Fransız Ceza Kanunu'nda interneti de içerecek şekilde "hangi yollarla veya araçlarla olursa olsun" gibi genel ifadeler kullanılarak bu suçların yaptırıma bağlanması tercih edilmiştir[335]. Bu şekilde düzenlemeler içerecek şekilde 1993'te çıkarılan Yeni Ceza Kanunu'nda bilişim sistemleri aracılığıyla kişilik haklarına saldırı, küçüklerin fotoğraflarının pornografide kullanılması, küçüklerce erişilebilecek şiddet ya da pornografi içeren mesajlar yayınlanması, 765 sayılı Eski Türk Ceza Kanunu'nun da esinlendiği bilişim sistemine hukuka aykırı erişim, verilerin silinmesi, değiştirilmesi ya da sistemin işlevinin değiştirilmesi, işletilmesinin engellenmesi, bilişim sistemi aracılığıyla dolandırıcılık fiilleri suç olarak düzenlenmiştir[336]. Sisteme ve veriye müdahale kapsamında ele alındığında; "bilgileri otomatik işleme tabi tutmuş bir sistemin fonksiyonunu bozucu veya engelleyici hareketlerde bulunmak ile sistemdeki bilgileri aldatıcı hareketlerle değiştirmek veya yok etmek" eylemlerinin suç olarak düzenlendiği görülmektedir[337]. 2000'lerde ise internette bulunan suç içerikli yayınların sorumlusunun kim olacağı sorunu bu konudaki tartışmaları gündeme getirmiş[338], bunun üzerine 1986 tarihli iletişim özgürlüğünü düzenleyen kanuna internet kişilerine ilişkin cezai yükümlülükler getirilmiştir[339]. Fransa 2008'de siber savunma konusunda bir dönüm noktası olan "Ulusal Savunma Beyaz Kitabı"'nı ilan etmiş, bununla askeri ve

---

[333] Yılmaz, "5237 Sayılı", 65.
[334] Rüya Şamlı, "Türk ve Dünya Hukukunda Bilişim Suçları", içinde *Akademik Bilişim '10 XII. Akademik Bilişim Konferansı Bildirileri*, editör Mustafa Akgül, Ethem Derman, Ufuk Çağlayan, Atilla Özgit, Tuğrul Yılmaz, (Muğla: Muğla Üniversitesi, 2010), 125.
[335] Turhan, "Bilgisayar Ağları ile", 93.
[336] Dülger, *İnternet İletişim Hukuku*, 235.
[337] Detaylı bilgi için bkz: Nacar, "Avrupa Birliği", 18 vd.
[338] Turhan, "Bilgisayar Ağları ile", 93.
[339] Dülger, *İnternet İletişim Hukuku*, 235.; Zeynel T. Kangal, "Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu". *Journal of Istanbul University Law Faculty* , 59/1-2 (2011): 229.; Ünver, "İnternet Açısından", 72.

savunma teşkilatını yeniden yapılandırarak aktif savunmada yeni bir dijital dönüşüm başlatmıştır[340].

1.5.4.3. Almanya

Almanya bilişim suçlarına ilişkin Kıta Avrupa'sında ilk düzenlemelerin ortaya konulduğu ülke olmakla beraber,[341] bu suçlar ayrı başlık altında ele alınmayıp, kanunda ilgili hükümlerin içerisine eklemelerde bulunularak, bu suçların düzenlemesi yoluna gidilmiştir[342]. Yapılan düzenlemelerde bilişim sistemindeki verilere erişim imkânı sağlamak, verilere yetkisiz olarak erişim yolu açmak, ağdaki verileri yetkisiz olarak yakalamak[343], verileri değiştirmek, bilgisayar sabotajı[344], bilişim sistemleri aracılığıyla sahtekârlık[345], banka ve kredi kartlarının kötüye kullanılması ve bunlarda sahtecilik[346] fiilleri yaptırıma bağlanmıştır. Alman Ceza Hukuku'nda bilişim sistemleri aracılığıyla sahtekârlık suçunun oluşmasında bir belgenin bilişim sistemleri aracılığıyla sahte olarak düzenlenmesi veya üzerinde tahrifat yapılması ve kullanılmasının yeterli görülmesi[347] ise kapsamı bakımından özellikle göze çarpan bir düzenlemedir. Alman hukuk sisteminde bilişim suçları ve bilişim yoluyla işlenen suçlar ceza kanunlarında düzenlenmiş olup, ayrıca bilişim teknolojileri kullanılarak işlenebilecek suçlara ilişkin özel kanunlarda da düzenlemeler mevcuttur[348].

Alman Ceza Kanunu m. 202b'de verilerin iletilirken hukuka aykırı bir şekilde ele geçirilmesi suç olarak düzenlenmiştir[349]. Buna göre yetkisiz bir kimsenin, teknik araçlardan yararlanarak, herkese açık olmayan bir veri iletiminde veya bilgi işlem donanımından yayılan elektromanyetik dalgalara girmek suretiyle verileri temin etmesi suç olarak düzenlenmiştir[350]. 303a/1'de verileri hukuka aykırı silme, erişilemez ya da

[340]Ahmet Emre Köker, "Ulusal Siber Güvenlik Stratejisi: Fransa", *UPA Strategic Affairs,* 3/1 (2022): 46.
[341] Dülger, *İnternet İletişim Hukuku,* 232.; Mahmutoğlu, "İnternet Süjelerinin", 43.
[342] Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", *Gazi Üniversitesi Hukuk Fakültesi Dergisi,* 14/2 ,(2010): 285.
[343] Erdağ, "Türk ve Alman Ceza", 285.
[344] Demircan, *Bilişim Alanında Suçlar,* 36.
[345] Dülger, *İnternet İletişim Hukuku,* 232.
[346]Erdağ, "Türk ve Alman Ceza", 297.
[347] Turhan, "Bilgisayar Ağları ile", 92.
[348] Akarslan, "Adli Bilişim Ayrımı", 113.
[349] Ulrich Sieber, "Bilişim Suçları", içinde *Bilişim Teknolojisi İle Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku (Yazarın Seçilmiş Makaleleri),* ed., Feridun Yenisey, Salih Oktar, Zehra Başer Doğan, (Ankara: Seçkin Yayıncılık, 2021), 298.
[350] Sieber, "Bilişim Suçları", 299.

kullanılamaz hale getirme veya değiştirme eylemleri suç olarak düzenlenmiş; 303a/2'de bunlara teşebbüs cezalandırılmıştır[351]. 303b'de ise sisteme hukuka aykırı giriş yoluyla mala zarar verme düzenlenmiş olup 303b/1'de failin başkası için önemli değer taşıyan bir bilgi işlem sürecinde 303/1'deki suçu işleyerek başkasına zarar vermek amacıyla sisteme veri dahil etmesi, veri iletmesi, bilgi işlem tesisatını ya da taşıyıcı cihazı tahrip etmesi, kullanılmaz hale getirmesi, yok etmesi veya değiştirmesi suç olarak düzenlenmiştir[352]. Bu suça teşebbüs ise ikinci fıkrada yer almaktadır[353]. Eğer bu bilgi işlem süreci bir işletme ya da makam bakımından önemli ise, bu durum, ağırlaştırıcı hal olarak öngörülmüştür[354]. 303b/4'de ise; yüksek miktarda malvarlığı kaybına yol açma, meslek haline getirme ya da temadi eder şekilde işlemek üzere oluşturulmuş bir çete mensubu olarak hareket etme, suça konu eylem ile toplum için hayati önem taşıyan malların teminine ya da halka hizmete engel olma ya da Almanya Federal Cumhuriyeti'nin güvenliğine zarar verme "çok ağır hal" olarak değerlendirilmiştir[355].

1.5.4.4. İtalya

İtalya 1993'te bilişim suçlarını İtalyan Ceza Kanunu'nda yer alan suçların içerisinde değişikliğe giderek eklemeyi uygun bulmuş, mala zarar verme suçlarına teknolojik cebir ve şiddet kavramı çerçevesinde bilişim programını tahrip etme, değiştirme, silme, bilişim veya telematik sistemin işlenmesini engelleme, bozma fiillerini eklemiş, kamusal yararı bulunan sistemlere yönelik zarar verme ve yok etme fiillerini ayrıca düzenlemeyi uygun bulmuş ve yetkisiz erişim, giriş kodlarının haksız elde edilmesi, bilişim sistemi, veri veya programlara zarar verme, işleyişini engelleme, özel olarak tahrip etme[356], bilişim belgelerinde sahtecilik, internet aracılığıyla küçüklerin pornografik materyallerde kullanılması, bilişim sistemleri aracılığıyla dolandırıcılık[357] suç olarak düzenlenmiştir. Ayrıca 1992'de çıkarılan kanunla kara para aklanmasıyla mücadelede hazırlık hareketlerini de cezalandıracak nitelikte yaptırımlar getirilmiştir[358].

[351] Sieber, "Bilişim Suçları", 299.
[352] Sieber, "Bilişim Suçları", 300.
[353] Sieber, "Bilişim Suçları", 300.
[354] Sieber, "Bilişim Suçları", 300.
[355]Sieber, "Bilişim Suçları", 300.
[356] Demircan, *Bilişim Alanında Suçlar*, 36-38.
[357] Dülger, *İnternet İletişim Hukuku*, 236.; Ünver, "İnternet Açısından", 72.
[358] Dülger, *İnternet İletişim Hukuku*, 236.

İtalyan Ceza Kanunu'nun m. 615ter'de kendine ya da başkasına yarar sağlamak ya da başkalarına zarar vermek amacıyla güvenlik sistemleri ile korunan bilişim sistemlerine erişim kodlarının hukuka aykırı elde edilmesi ve yayılması[359]; 615quinques'de virüs programlarını kasten yayan kişilerin eylemlerinin engellenmesi hedeflenerek, bir bilişim veya telematik sistem içerisinde saklı program ve verilere zarar verme ya da sistemin işleyişini tamamen yahut kısmen engelleme veya bozma amacıyla ya da bunları sonuç olarak gerçekleştirecek kendi ya da başkası tarafından yazılan bilişim programını bildiren veya veren kişinin fiilinin cezalandırılacağı düzenlenmiştir[360]. Ayrıca 615ter'de sisteme girme ve kalma eylemi açısından kamu görevlisi failin kamusal sıfatını kötüye kullanarak eylemi gerçekleştirmesi halinin ağırlatıcı neden sayıldığı; 617ter'de ise sisteme girme ve müdahale eylemlerinin devlet, kamu kuruluşu veya kamu hizmeti gören kuruluşların sistemlerine karşı kamu görevlisi tarafından kamusal sıfatını kötüye kullanarak eylemi gerçekleştirmesi halinin yine ağırlatıcı neden sayıldığı görülmekte olup[361], ülkemizde halen daha düzenleme eksikliği görülen konular olması açısından dikkat çekicidir.

1.5.4.5. İngiltere

Anglo-Sakson hukuk sisteminin genel özelliklerinden bağımsız bir şekilde bilişim suçlarını ayrı bir kanunda düzenleyen İngiltere, 1990'larda 3 bölüm ve 18 kısımdan oluşan; bilgisayarlara, verilere ve programlara yetkisiz erişim ve veri ve programların yetkisiz değiştirilmesine ilişkin suçları düzenlediği Bilgisayarın Kötüye Kullanılması Kanunu'nu çıkarmıştır[362]. Ana bölümlerin ilkinde suç tipleri, ikincisinde ceza muhakemesine ilişkin hükümler, üçüncüsünde ise konuya dair bazı genel düzenlemeler getirildiği görülmektedir[363]. Sisteme ve veriye müdahale kapsamında ele alındığında, kanunda; bilgisayar veri ve programlarının yetkisiz olarak değiştirilmesi, verileri silmek, kasti olarak arıza oluşturmak için sisteme virüs sokmak[364] eylemlerinin suç olarak düzenlendiği görülmektedir. Bu kanun dışında bilişim sistemleriyle işlenen dolandırıcılık, müstehcenlik, sahtecilik, ekstrem pornografi, grooming, kişisel verilere

[359] Yılmaz, "5237 Sayılı", 65.
[360] Carlo Sarzana di S. Ippolito, "Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması İtalya'daki Durum", çev. Vesile Sonay Daragenli, *İstanbul Hukuk Fakültesi Dergisi*, LV/3 (1997), 401.
[361] Ünver, "İnternet Açısından", 67-69.
[362] Ermeydan, *Bilişim Suçları*, 89.; Dülger, *İnternet İletişim Hukuku*, 233.
[363] Akarslan, "Adli Bilişim Ayrımı", 112.
[364] Detaylı bilgi için bkz: Nacar, "Avrupa Birliği", 23-25.

ilişkin eylemlere yönelik suç tipleri de düzenlenerek kanunlaştırılmış, ayrıca AKSSS'ye taraf olması dolayısıyla da sözleşme kapsamında kanunlarında çeşitli değişiklikler yapmıştır[365]. 1964 tarihli Müstehcen Yayınlar Kanunu ile 1984 tarihli Telekomünikasyon Kanunu'nda yayınlama terimi kapsamına veriler de dahil edilerek sanal alemde yapılan pornografik yayınlar düzenlenmiş[366], 1978 tarihli Çocukların Korunması Kanunu'nda yer alan fotoğraf tanımında dijital fotoğrafları da içerecek şekilde değişiklik yapılarak çocuk pornografisi resimlerini ve montajlarını bulundurmak suç haline getirilmiştir[367].

1.5.4.6. Japonya

Korunan hukuksal değeri dikkate almak suretiyle düzenlemeler oluşturan Japonya'da 1987'de Ceza Kanunu'nda değişikliğe giderek bilişim suçlarına ilişkin hükümler eklemiş, 2000'lerde ise "İnternete Haksız Girmenin Yasaklanması Hakkındaki Kanun" adlı kanun çıkarılmıştır[368]. Teknolojik gelişmelerin merkezinde bulunan Japonya erken yıllarda bilişim suçlarına karşı tedbirler almış ve 2001'de AKSSS'yi imzalayarak mevzuatında sözleşmeye paralel şekilde yasal düzenlemeler oluşturmuştur[369].

1.5.4.7. Uluslararası Düzenlemeler

Bilgisayar ağlarının gelişimi dünyayı birbirine bağlayan bir bilgi ağı kurmakla beraber, bir yandan da bilişim suçlarının dünyanın bir ucundan diğer ucuna etki edebilecek şekilde işlenebilmesine de imkân tanımıştır. Bu durum üzerine ilk başlarda ülkesel bazda işlenen bilişim suçları, küreselleşme ile beraber milletlerarası bir boyut kazanmış, dünya çapında yayılan bu suçların tanımından yaptırımına kadar her ülkede farklılık göstermesi, devletlerin uluslararası işbirliğinin etkin bir şekilde yürümesini engellemiş ve işlenen fiillerin cezalandırmasını zorlaştırmış, böylece de ortaya çıkan tüm bu sorunlarla, bilişim suçları, uluslararası ceza hukukunu ciddiyetle ilgilendirir bir hale

[365] Ermeydan, *Bilişim Suçları*, 46.; Dülger, "Karşılaştırmalı Hukuk Bağlamında", 247.
[366] Akın Aytekin, Mehmet Serkan Kılıç ve Hüseyin Çakır, "Karşılaştırmalı Hukuk Açısından Siber Suçlar", içinde *Güncel Tehdit: Siber Suçlar*, ed., Hüseyin Çakır ve Mehmet Serkan Kılıç, (Ankara: Seçkin Yayınları, 2014), 197.
[367] Aytekin, Kılıç ve Çakır, "Siber Suçlar", 197.; Mahmutoğlu, "İnternet Süjelerinin", 48.
[368] Akarslan, "Adli Bilişim Ayrımı", 115.; Esra Yaycı, "Bilişim Suçları", (Yüksek Lisans Tezi, Gazi Üniversitesi, 2007), 61.; Ünver, "İnternet Açısından", 76.
[369] Ermeydan, *Bilişim Suçları*, 90.

gelmiştir[370]. Gerçekten de bilişim suçları açısından failin bir ülkeden istediği herhangi farklı bir ülkeyi ya da farklı ülkedeki kişiyi hedef alma imkanına sahip olması uluslararası işbirliğini mecburi kılmakta, herhangi bir devletin işbirliğine katılmaması halinde failin o ülkeler üzerinden faaliyetlerini devam ettirmesine imkan sağlayacağından, bu durumda doktrinde ifade edildiği şekliyle bu suçlarla mücadele ya global olacak ya da mücadelenin anlamı bulunmayacaktır[371].

Mukayeseli hukukta bilişim suçlarının tanımının net bir şekilde ifade edilmemesi ve yeknesak bir düzenlemenin mevcut olmaması, teknolojik gelişmelerin hızına yetişemeyen mevzuatların gelişmeleri geriden takip etmesi, klasik suç tiplerinin bilişim suçlarını tam anlamıyla kapsayacak nitelikte olmaması, bu suçların tespitinin diğer suçlara göre oldukça zorlayıcı olması, bilişim suçlarında fail ile mağdur arasında mekânsal mesafenin genişliği ve bu suçların sınır tanımazlığı, bu suçların birden fazla ülkede gerçekleştirilmesi durumunda suçun işlendiği yer sorununun ortaya çıkması, uluslararası adli yardımlaşmanın gerektiği hallerde bu yardımlaşmanın karmaşık ve yavaş işleyen resmi prosedürler içermesi gibi birçok sebeple bu suçlarla mücadelede uluslararası düzenlemeler yapılarak adli yardımlaşmanın sağlanması şart olmuş ve bu sorunları çözebilmek için bu konuda geniş çaplı adımlar atılmıştır[372].

Sayılan tüm bu sorunları çözebilmek ve devletlerarası adli yardımlaşmayı etkin bir şekilde sağlamak amacıyla Birleşmiş Milletler, G-8, OECD, Avrupa Konseyi gibi birçok uluslararası organizasyon üst seviyede bir hukuki düzenleme ortaya koymak adına birçok çalışma gerçekleştirmiştir[373]. Bu konuda uluslararası alanda bilişim suçlarına karşı çözüm arayışları ilk olarak 1980'li yıllarda Birleşmiş Milletler Suçların Önlenmesi ve Suçluların Tretmanı Kongreleri ile yapıldığı görülmüştür[374]. Yine bu alanda atılan adımlardan biri de Avrupa Komitesi'nin 1996'da Avrupa Konseyi'ne tavsiyesi üzerine 1997'de kurulan "Siber-uzay Suçları Uzman Komitesi" (Committee of Experts on Crime in Cyber-space) tarafından 2001 yılında hazırlanarak aynı yıl Budapeşte'de imzaya açılan ve 2004 yılında yürürlüğe giren Avrupa Konseyi Siber Suç

[370] Dülger, *İnternet İletişim Hukuku*, 198.
[371] Aliusta ve Benzer, "Dahil Olma Süreci", 37.
[372] Detaylı bilgi için bkz: Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 19/2 (2013), 1232 vd.
[373] Turhan, "Bilgisayar Ağları ile", 75.
[374] Ermeydan, *Bilişim Suçları*, 80.

Sözleşmesidir[375]. Avrupa Konseyi üyesi olmayan birçok devlet tarafından da kabul edilen bu sözleşme bu alandaki ilk uluslararası sözleşme olma niteliğini taşımaktadır[376].

Budapeşte Sözleşmesi olarak da anılan Avrupa Konseyi Siber Suç Sözleşmesi'nin (AKSSS) başlıca amaçları; ortak tanımlamalarda bulunmak suretiyle ulusal mevzuatların uyumunu sağlamak, soruşturmada ortak yetkileri belirleyerek muhakeme kurallarını yeknesaklaştırmak, yeni işbirliği yöntemleri ortaya konarak hükümlerin uygulanmasını hızlandırmak şeklinde ifade edilmektedir[377]. Bu amaçları gerçekleştirmek için ortaya konan AKSSS içeriğinde sırasıyla; terimlerin kullanımı, ulusal düzeyde alınacak önlemler, uluslararası işbirliği ve diğer hükümler olmak üzere dört bölüm ve bu bölümlerin içerisinde yer alan toplam kırk sekiz maddeden ihtiva edilmiştir. Birinci bölümde yer alan birinci maddede bilgisayar sistemi, bilgisayar verisi, servis sağlayıcı ve veri trafiği kavramlarının tanımı yapılmış, ikinci bölüm ise esas ceza hukuku, usul hukuku ve yargı yetkisi olmak üzere üç kısma ayrılmıştır[378].

Sözleşmenin ikinci bölümünde ilk kısımda maddi ceza hukuku düzenlenmiş olup 2-13. maddeler arasında belli başlı suç tiplerinin düzenlendiği görülmektedir. Burada suç olarak düzenlenen eylemler asgari düzeyde belirlemeleri içermekte olup büyük ölçüde Avrupa Konseyi'nin R(89)9 sayılı tavsiyesi çerçevesinde geliştirilen talimatlar ile diğer kamusal ve özel kuruluşların çalışmaları esas alınarak ortaya konmuştur[379]. Burada düzenlenen suç tipleri belli başlıklar altında ayrılmaktadır. İlk başlık sistem ve veri gizliliği, bütünlüğü ve bu veri ve sistemlerin kullanıma açık bulunmasına yönelik fiilleri içeren maddelerden oluşmakta ve bu başlık altında yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale ve cihazların kötüye kullanımı fiilleri suç olarak düzenlenmiş olup, taraf devletlere gerekli usule yönelik işlemlerin yapılması konusunda yükümlülük getirmektedir. İkinci başlık bilgisayarlarla ilişkili suçları düzenlemekte olup, bilgisayar aracılığıyla işlenen sahtecilik ve dolandırıcılık suçlarını ele almaktadır. Üçüncü başlık ise çocuk pornografisine ilişkin hükümler içeren içeriğe ilişkin suçlar olarak düzenlenmiştir. Bu düzenleme doktrinde internetin ortaya çıkışıyla hızla artış

[375] Önok, "Uluslararası İşbirliği", 1241.; İçel, "Avrupa Siber Suç", 6.
[376] Dülger, *İnternet İletişim Hukuku*, 209.
[377] Önok, "Uluslararası İşbirliği", 1242.; İçel, "Avrupa Siber Suç", 6.
[378] "Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001", (E. T. 15.01.2025) https://www.coe.int/en/web/cybercrime/the-budapest-convention
[379] Turhan, "Bilgisayar Ağları ile", 102.; İçel, "Avrupa Siber Suç", 7.

gösteren çocuk pornografisin eylemlerine karşı mücadelede hukuksal bağlamda oldukça önemli bir gelişme olarak görülmüştür[380]. Dördüncü başlıkta telif hakkı ve benzeri hakların ihlaline ilişkin suçlar düzenlenmişken; ilave yükümlülük ve yaptırımlar adlı beşinci başlıkta ise teşebbüs, yardım ve yataklık, tüzel kişilere yönelik yaptırımlar gibi hususlar değerlendirilmiştir. Sözleşmede suç olarak düzenlenen eylemlerin ortak özelliği eylemin hak sahibi olunmadığı halde gerçekleştirilmesi ve kasten gerçekleştirilmesi olup söz konusu eylemler rıza, meşru müdafaa ya da zaruret hali gibi durumlarda kapsam dışı bırakılacak ve örneğin; kamu düzenini sağlama, suç soruşturması ve kovuşturması ya da ulusal güvenliği koruma gibi amaçlarla eylemin gerçekleştirilmesi halinde, eylem suç kapsamı dışında kalacaktır[381].

İkinci bölümün ikinci kısmında ise devletlerin birinci kısımda belirtilen fiilleri yaptırıma bağlamak için gerekli yasama işlemlerini yapmasını ve ilgili kısımda belirtilen saklanan bilgisayar verileri ile trafik bilgilerinin korunması, arama ve el koyuma gibi konularda gereken önlemleri yerine getirmesini talep etmekte, üçüncü kısımda ise yargı yetkisini ele almaktadır. İkinci kısımda düzenlenen önlemler bir bilişim sistemi vasıtasıyla işlenen ya da elektronik deliller içeren her tür suç için geçerli bulunduğundan kapsamı ilk kısımda düzenlenen suçlardan daha geniştir[382].

Sözleşmenin Uluslararası İşbirliği başlıklı üçüncü bölümünde sözleşmeye taraf olan devletlerin mümkün mertebede en geniş şekilde adli yardımlaşmayı sağlaması ve bu konudaki engelleri en az düzeye indirmesi istenmekte olup, sadece siber suç fiilleri konusunda değil, aynı zamanda elektronik şekilde delil toplanmasını gerektiren klasik suç tiplerini de içerecek şekilde bir adli yardımlaşmayı öngörmekte ve uluslararası adli yardımlaşmaya ilişkin genel ilkeleri belirlenmektedir[383]. AKSSS'nin "İnternet Ortamında Ceza Sorumluluğunun Avrupa Ana İlkeleri" olarak adlandırılan dört ana ilkeden oluştuğu ifade edilmekte olup; bu ilkelerden ilki, ceza sorumluluğunun

[380] Murat Volkan Dülger, "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler", *İstanbul Barosu Dergisi*, 4 (2004): 8. https://www.researchgate.net/publication/349573730_Avrupa_Konseyi_ve_Avrupa_Birligi_Duzenlemelerinde_Cocuk_Pornografisinin_Internet_Araciligiyla_Yayilmasina_Karsi_Yapilan_Duzenlemeler.; Füsun Sokullu Akıncı, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi", *Journal of Istanbul University Law Faculty*, 59/1-2 (2011): 31.
[381] Turhan, "Bilgisayar Ağları ile", 103.; İçel, "Avrupa Siber Suç", 8.
[382] Turhan, "Bilgisayar Ağları ile", 104.
[383] Önok, "Uluslararası İşbirliği", 1249.

belirlenmesinde iletişim özgürlüklerinin gereklerine uyulması, ikincisi suçların belirlenmesinde ortak bir minimum standarda uyulması, üçüncüsü hukuka aykırı bir fiil olması, dördüncüsü fiilin kasten gerçekleştirilmesidir[384].

AKSSS her ne kadar dünya genelinde birçok devlet tarafından kabul edilmiş bir sözleşme olsa da bu sözleşmenin bazı konularda eleştiri topladığı da görülmüştür. Bu eleştirilerden ilki sözleşmede değişiklik yapılmasına ilişkin hükümler içeren sözleşmenin 44. Maddesinde yer alan zorlu koşullar içermesi nedeniyle, değişiklik yapılması gereken durumlarda sözleşmenin siber suçların değişkenlik hızına uyum sağlayamayacağı yönündedir[385]. Maddeye göre sözleşmede değişiklik yapılabilmesi için; değişiklik teklifinin üye, üye olmayan ancak hazırlanmasında payı bulunan ve üye olmaya davet edilen ülkelere bildirilmesi, teklif edilen değişikliklerin komisyona bildirilmesi, değişikliğe ilişkin görüşün komisyonca kurula sunulması ve kurulca değerlendirilmesi, tekrar taraflarla görüş alışverişi yapılması, son olarak kabul için taraflara gönderilmesi ve tarafların tamamının kabulünün bildirilmesinden sonraki 30. günde yürürlüğe girmesi öngörülmektedir[386]. Dolayısıyla değişikliğin gerçekleştirilebilmesi için uzun bir prosedür gerektiğinden, bu durum, sözleşmenin siber suçlarla mücadelede geride kalarak güncelliğini koruyamamasına neden olabilecektir. Yine bunun yanında sözleşme hazırlanırken gelişmekte olan devletlerle sivil toplum kuruluşlarının görüşlerine yeterli yer verilmediği; sözleşmenin çekincelere genişlik tanıyan hükümleri sebebiyle taraf devletlerin ulusal hukuklarını sözleşmeye uyumlaştırma gereği hissetmemeleri durumunda, bu durumun uluslararası işbirliğini zorlaştıracağı; sözleşmeyle internet servis sağlayıcılarına getirilen yüklerin oldukça ağır olduğu konuları da eleştiri konusu olmuştur[387]. Ancak sonuç itibariyle AKSSS, taraf devlet sayısının çokluğu ve bilişim suçlarıyla mücadelede uluslararası işbirliğinin sağlanmaya yönelik attığı adımlar açısından oldukça önemli bir yere sahiptir.

[384] Akarslan, "Adli Bilişim Ayrımı", 119.; İçel, "Avrupa Siber Suç", 6-8.
[385] Önok, "Uluslararası İşbirliği", 1245.
[386] "Convention on Cybercrime".
[387] Bu konuda detaylı bilgi için bkz: Önok, "Uluslararası İşbirliği", 1245.

Ülkemizde ise AKSSS 10 Kasım 2010'da imzalanmış olmakla birlikte uzunca bir süre sürüncemede bırakılmış, nihayet 2014 yılında onaylanıp yürürlüğe girmiş ve sonuç itibariyle Türkiye 1 Ocak 2015'ten itibaren sözleşmeye taraf olmuştur[388].

Bilişim suçlarıyla uluslararası mücadelede suçun işlendiği yerin belirlenmesindeki zorluk ve pek çok önemli siber saldırının geçen yıllarda araştırılmamış olması BM'nin Enternasyonal Telekomünikasyon Birliğine araştırma görevi vermesi ile sonuçlanmış; bunun üzerine 2007'de uzmanlardan oluşan bir çalışma grubu kurularak çözüm önerileri geliştirilmiştir[389]. Bu çalışma grubunun en önemli tavsiyesi ise siber suçların yargılama yetkisi bulunmayan mevcut Uluslararası Ceza Mahkemesi örnek gösterilerek, bu mahkeme bünyesinde yer almayan ancak siber suçlarla mücadelede buna benzer bir mahkemenin kurulmasının sorunların çözümünde etkili olacağına yöneliktir[390].

1.5.5. Türk Ceza Kanununda Bilişim Alanında Suçlar Bölümünde Düzenlenen Suçlar

Bilişim suçlarının hukukumuza girişi 765 sayılı eski Türk Ceza Kanunu ile 1991 yılında gerçekleşmiş, söz konusu kanunda yer alan hükümler 01.06.2005'te yürürlük kazanan 5237 sayılı Türk Ceza Kanunu'na kadar uygulama alanı bulmuştur[391]. 765 sayılı eski TCK sistematiğinde suç tipleri devlete – topluma – kişilere ve mala karşı işlenen suçlar şeklinde sıralama bularak korumada devleti öncelik alan bir yaklaşıma sahipken 5237 sayılı TCK'da bu sistem terk edilerek insanlıktan devlete doğru bir sıralama yapılmış ve bireyciliği ön plana çıkaran bir yöntem izlenmiş olmakla beraber[392] her iki kanun açısından da ortak bir şekilde suçlar koruduğu hukuki değer gözetilerek tasnif edilmiştir[393]. Ancak her iki kanun açısından da bilişim suçlarının düzenlenmesinde hukuki değere göre tasnif yapılmadığını ve bu sebeple de bu suçlar açısından yapılan düzenlemenin kanun sistematiğini bozduğu yönünde eleştiriler getirilmiştir[394]. Bunun

[388] Erkan, "Bilişim Sistemine", 36.
[389] Sacit Yılmaz, *Türk Ceza Hukuku Sisteminde Siber Suçlar,* (Ankara: Adalet Yayınevi, 2023), 158.
[390] Yılmaz, *Siber Suçlar,* 159.
[391] Akarslan, *Bilişim Suçları*, 43.; Levent Kurt, *Açıklamalı - İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* (Ankara: Seçkin Yayıncılık, 2005), 116.
[392] Mustafa Avcı, "TCK, Tasarılar ve 2004 TCK Tasarısı'nın Genel Olarak Değerlendirilmesi", içinde *Türk Ceza Kanunu Reformu İkinci Kitap Makaleler, Görüşler, Raporlar*, ed. Teoman Ergül, (Ankara: Türkiye Barolar Birliği Yayınları, 2004.), 211.
[393] Akbulut, *Bilişim Alanında Suçlar*, 102 vd.
[394] Bu konuda detaylı bilgi için bkz: Akbulut, *Bilişim Alanında Suçlar*, 102 vd.

sebebi ise bilişim suçlarının her iki kanunda da aynı başlık altında bir arada düzenlenmesi ve farklı hukuki değerleri koruyan hükümlerin bir araya toplanmış olmasıdır. Bu durumun söz konusu hükümler yorumlanırken probleme yol açacağı ve hükümler açısından hangi hukuki değerin kabul edilmesi gerektiğinin tespit edilememesine yol açacağı düşünülmektedir[395]. Bu eleştirilere karşılık bilişim alanında suçların ayrı bir başlık altında toplamasının uygulamacıya kolaylık sağladığı ve bu sebeple de sistematiğe uygun bir şekilde düzenlenmemesinin yerinde olduğunu dile getiren görüşler de vardır[396].

Bilişim suçlarına yönelik mevzuatımızda geniş kapsamlı düzenleme getirilmiş ve mevcut düzenlemeler genel olarak hem mevzuat yönünden hem de işleyişte oturtulmuş durumda bulunuyor[397] ise de bazı konularda eksiklerin olduğu ve yeni düzenlemelere ihtiyaç olduğu da doktrinde tartışılmaktadır. İlk olarak; siber zorbalık eylemlerine karşı TCK'nın yetersiz kaldığı noktasındadır. Zorbalığın sosyal medya üzerinden yaşatılan türü olarak da değerlendirilebilen[398] siber zorbalık, bilgi ve iletişim teknolojileri kullanılarak bir kişi ya da grup tarafından, başka bir kimseye ya da başka bir topluluğa karşı kasıtlı olarak icra edilen, tekrarlayan saldırgan davranışlar içeren, teknik veyahut ilişkisel zarar verme eylemlerinin tamamıdır[399]. Siber gözetleme, siber ırkçılık, sosyal medya aracılığıyla taciz, hakaret, şantaj, kullanıcıyı devamlı olarak rahatsız etme, rızası hilafına kullanıcının hesabını takip etme ve profiline ısrarla bakma gibi mağdura psikolojik açıdan zarar veren eylemler siber zorbalık olarak değerlendirilmektedir[400]. Dünyada bazı ülkelerce siber zorbalık eyleminin suç olarak düzenlendiği ve yaptırıma bağlandığı ancak Türkiye'de bu fiillere ilişkin özel bir düzenleme bulunmadığından bu tarz eylemlerin eğer koşulları mevcutsa TCK'da ilgili maddelere göre cezalandırıldığı ve bu sebeple de bu fiillere karşı yeterli koruma sağlanamadığı düşünülmektedir[401]. Bir diğer konu ise; yapay zekâ teknolojisinin gelişmesiyle birlikte, yapay zekânın kışkırtıcı

[395] Akbulut, *Bilişim Alanında Suçlar,* 103. Önder, *Şahıslara ve Mala,* 506.
[396] Demircan, *Bilişim Alanında Suçlar,* 64.
[397] Akarslan, *Bilişim Suçları,* 43.
[398] Şaban Cankat Taşkın, Stalking (Siber Gözetlenme) Eyleminin Ceza Hukukundaki Yaptırımının Değerlendirilmesi, İçinde Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı, ed. Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar, (Ankara: Adalet Yayınevi, 2021), 292.
[399] Hüseyin Serin, "Ergenlerde Siber Zorbalık/ Siber Mağduriyet Yaşantıları ve Bu Davranışlara İlişkin Öğretmen ve Eğitim Yöneticilerinin Görüşleri" (Doktora Tezi, İstanbul Üniversitesi, 2012), 21.
[400] Taşkın, Stalking, 292.
[401] Taşkın, Stalking, 310.

ve ayrımcı şekilde kullanılmasına ilişkin örnek vakaların ortaya çıkmaya başladığı ve bu durumun insan hakları ile toplum açısından bir tehdit oluşturduğu, bu tehdidin önüne geçebilmek içinse yapay zekânın ulusal ve uluslararası düzeyde korunan ayrımcılık yasağına aykırı amaçlarla kullanılmasının yaptırıma bağlanması gerektiği konusunda düşünceler mevcuttur[402].

Kanunda bilişim suçlarına yönelik olarak yapılan düzenlemelerin bir noktada yetersiz hale gelmesi ve tartışmaların ortaya çıkması, teknolojinin bilişim dünyasındaki gelişimi ve sosyal hayattaki yoğunluğuna bağlı olarak son derece doğal bir süreç olup ilerleyen süreçte bu konuda yeni sorunların ortaya çıkması kaçınılmazdır. Bu sebeple de bilişim suçlarına ilişkin yapılacak düzenlemelerin zamanın akışına uygun ileri görüşlü bir şekilde düzenlenmesi ve geleceğe yönelik olmasında fayda vardır. Bu noktada önem arz eden; konuyla ilgili mukayeseli hukuktaki çalışmaların takip edilerek karşılaşılabilecek sorunların belirlenmesi ve geç kalmadan önlem alınması, iç hukuktaki sorun tespit edildikten sonra ise hızlı bir şekilde müdahale edebilmek amacıyla gerekli düzenlemelerin oluşturulmasıdır. Bu konuda özellikle uluslararası anlaşmaların etki değeri büyük olup Türkiye'nin de taraf olduğu AKSSS bu konuda oldukça önem arz etmektedir.

AKSSS'de 14-21 maddeleri arasında yer alan usul hukuku düzenlemeleri açısından doktrinde 5271 sayılı Ceza Muhakemesi Kanunu'nun oldukça yetersiz ve eksik olduğu, sözleşmede düzenlenen "depolanan bilgisayar verisinin süratli şekilde korunması", "Trafik verisinin süratli şekilde korunması ve kısmen açıklanması", "trafik verilerinin gerçek zamanlı toplanması", "içerik verilerinin takibi" tedbirlerinin Türk hukukunda bir karşılığının olmadığı, "üretim emri" ile "depolanmış bilgisayar verilerinin aranması ve bunlara el konulması" tedbirlerine karşılık Türk hukukunda 5271 sayılı Kanun m. 134 bulunsa da uygulamada oldukça eksik ve sorunlu bir düzenleme olduğu ve tüm bu hususlar birlikte değerlendirildiğinde Türk ceza muhakemesi hukukunun bilişim suçlarına yönelik usul bakımından oldukça geri kaldığı ifade edilmektedir[403].

[402]Bu konuda detaylı bilgi için bkz: Murat Balcı, "Yapay Zeka ve Ayrımcılık", İçinde Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı, ed. Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar, (Ankara: Adalet Yayınevi, 2021), 332 vd.
[403] Aliusta ve Benzer, "Dahil Olma Süreci", 40.

Bilişim suçlarının içerik düzenlemesinde ise AKSSS sistemine paralel bir şekilde yapılmış olan 5237 sayılı Kanunda, sözleşmede olduğu gibi, bilişim suçunun tanımı yapılmayarak eylemler temel alınmak suretiyle bilişim suçları yaptırıma bağlanmıştır. Öğretide doğrudan (Gerçek Bilişim Suçları) ve dolayısıyla (Bilişim Bağlantılı Suçlar) olmak üzere ikiye ayrılarak incelenen bilişim suçları ayrımı 5237 sayılı TCK'da da kabul edilmiş ve bu kalıba uygun bir biçimde düzenleme yapılmıştır[404]. 5237 sayılı TCK'da yer alan düzenlemeye göre doğrudan bilişim suçları kanunun 10. Bölümü olan "Bilişim Alanında Suçlar[405]" bölümünde m. 243 ile m. 245 arasında düzenlenmiştir. Dolaylı bilişim suçları ise kanununun ilgili muhtelif yerlerinde hırsızlık, dolandırıcılık gibi diğer suçların içerisinde düzenleme bulmaktadır. Bu şekilde dolaylı bilişim suçlarının düzenlenmesiyle kanun koyucu klasik/geleneksel suç tiplerine ilişkin norm ihlallerini düzenlerken, suçların işleniş şekillerini çeşitlendirerek, bilişim suçlarına vücut veren yeni fiiller eklemiştir[406]. Bununla birlikte bilişim suçları yalnızca TCK'da değil, TCK dışında 5070 sayılı Elektronik İmza Kanunu, 2499 sayılı Sermaye Piyasası Kanunu ve 5846 sayılı Fikir ve Sanat Eserleri Hakkında Kanun gibi diğer kanunlarda yer almaktadır[407]. Bu kapsamda örneğin TCK m. 142/2-e'de hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi düzenlenmiş ve bu şekilde faillerin teknolojik gelişmelerin sağladığı kolaylıktan faydalanılması bir nitelikli hal olarak görülmüştür[408]. Böylece kanun, bilişim sistemlerinin suçta kullanılmasının; faillerin suç işlemesini kolaylaştırma, suç işlendikten sonra suçun failinin belirlenmesini zorlaştırma gibi soruşturma ve kovuşturmaya yönelik yaşattığı zorluklara karşı caydırıcı ve koruyucu tedbirler alma yoluna giderek, genel hatlarıyla uluslararası düzenlemelere paralel bir şekilde teknolojik gelişmeleri kabul eden bir yaklaşım oluşturmuştur.

AKSSS düzenlenmesine de paralel bir şekilde oluşturulan ve öğretide doğrudan bilişim suçları olarak adlandırılan bilişim suçlarının Türk Ceza Kanunu'nda "Topluma Karşı

[404] Yargıtay Ceza Genel Kurulu, 17.11.2009, E. 2009/11-193 K. 2009/ 268, https://www.kazanci.com.tr/, E. T. 15.01.2025.
[405] Doktrinde bölüm başlığında yer alan "bilişim alanı" ifadesi yerine "bilişim sistemi" teriminin kullanılmasının daha yerinde olacağı yönünde görüşler de mevcuttur. İlgili görüş için bkz: Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1016.
[406] Eker, "Eski TCK Bağlamında", 120.
[407] Karipçin, "Sistemi Engelleme, Bozma", 51.
[408] Gül, *Doğrudan – Dolaylı*, 358.

Suçlar[409]" başlıklı üçüncü kısmının "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde düzenlendiği görülmektedir. Bu bölümün içerisinde, Bilişim Sistemine Girme ve Veri Nakillerini İzleme (TCK m. 243), Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (TCK m. 244), Banka veya Kredi Kartlarını Kötüye Kullanma (TCK m. 245), Yasak Cihaz ve Programların Bulundurulması ve Kullanılması (TCK m. 245/A) suçları düzenlenmiş olup yaptırıma bağlanmıştır:

1.5.5.1. Bilişim Sistemine Girme Suçu (TCK m. 243) ve Veri Nakillerini İzleme Suçu (TCK m. 243/4)

TCK m. 243/1'e 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.*" denilmek suretiyle bilişim sistemine hukuka aykırı olarak girmek veya orada kalmaya devam etmek suç olarak düzenlenmiştir. 765 sayılı eski TCK'da verilerin ele geçirilmesi suçu düzenlemesinde sisteme hukuka aykırı girişin yaptırıma bağlanmaması maddeye getirilen en önemli eleştirilerden biri iken yapılan düzenlemeyle bu sorun ortadan kalkmıştır[410].

Sisteme girmekle kastedilen sistemin donanımsal bölümüne girmek değil sisteme erişim olup Avrupa Komisyonu bilgisayar sistemlerinin bir bölümüne ya da tümüne yapılan hukuka aykırı erişimleri "izinsiz erişim" olarak ifade etmektedir[411]. Bu kapsamda örneğin bilgisayar kasasını açmak gibi sisteme fiziki müdahale yoluyla yapılacak eylemler girme olarak değerlendirilmeyecektir[412]. Sisteme e-posta veya dosya gönderilmesi yalnızca veri göndermeyi ifade ettiğinden sisteme girme kapsamında değilken, bilgisayarın işletim sistemine rıza olmaksızın girilmesi sisteme girme suçunu oluşturur[413]. Sistemlerin herkes tarafından kolaylıkla erişilebilecek sistemler olması halinde, diğer bir ifadeyle, örneğin bir kütüphanenin sistemi veya herkesin rahatlıkla

[409] Doktrinde bu suçlarla korunan hukuki yararın bilişim sistemlerine duyulan güven duygusu olduğundan bu kısımda düzenlendiği düşünülmektedir. İlgili görüş için bkz: Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 991.
[410] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku,* 1026.
[411] Nevzat Özsoy, "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK 243 ve 244)", *Yaşar Hukuk Dergisi,* 1/2 (2019), 304.; Yavuz Erdoğan, "Türk Ceza Kanununda Bilişim Sistemini Engelleme Bozma Verileri Yok Etme Değiştirme Suçu", (Doktora tezi, Marmara Üniversitesi, 2011), 110.
[412] Kayaer, "Bilişim Sistemine Girme", 102.; Şaban Cankat Taşkın, "Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları", (Yüksek Lisans Tezi, Marmara Üniversitesi, 2008), 29.
[413] Özsoy, "Doğrudan Bilişim Suçları", 305.

ulaşabileceği bir web sitesi gibi herkes tarafından istenilen anda erişilebilen bir sistem olması halinde, yani erişimde kişi bazında bir kısıtlama olmaması durumunda, söz konusu suç oluşmayacaktır[414]. Buna göre TCK m. 243/1'in oluşabilmesi için sisteme erişimin tedbirlerle sınırlandırılmış olması ve erişim yetkisinin usule uygun şekilde verilmesi asgari aranması gereken hususlardır[415], ancak bununla birlikte; sistemde şifre olmaması hali sisteme herkesin erişimine zımnen rıza gösterildiği anlamına da gelmemektedir[416]. Sistemde kalan kişinin mutlak surette sisteme giren kişi olması gerekmez; sisteme hukuka aykırı giren kişi farklı bir kişi olsa bile, sistemde kalmaya devam eden kişi de bu suçu işlemiş olur[417]. Bilişim sistemine izinsiz giriş suç oluşturmakla birlikte; ilgilinin rızası ve kanun hükmünün icrası hukuka uygunluk nedenleri bulunabileceği gibi, somut olaya göre suç tipi açısından hata hükümlerinin uygulanması da söz konusu olabilir[418]. Sisteme giriş birden fazla kişinin hukuken korunan haklarını ihlal ediyorsa, örneğin; bir kimsenin kişisel dosyası başkasının sisteminde saklanıyorsa ve fail sisteme girerek bu dosyaya ulaşırsa, bu kişilerin hepsi mağdur sıfatını kazanacak, yine sisteme giriş konusunda birden fazla kişinin yetkili bulunduğu hallerde yetkili herkes suçta mağdur konumunda olacaktır[419].

TCK m. 243/1 ile bilişim sisteminin güvenliği koruma altına alınmak istenmekte olup[420], toplum düzeni, kişisel veriler ve özel hayatın gizliliği, haberleşmenin gizliliği, kullanıcıların ve sistem üzerinde hak sahibi olanlar korunmakta[421], emniyet duygusu gibi farklı çıkarları koruma altına alınmakta[422] ve diğer bilişim suçlarının engellenmesi ile bilişim sistemleri ile programlarının güvenliğinin sağlanması amaçlanmaktadır[423]. Fıkranın ilk halinde sisteme girme fiili ile sistemde kalmaya devam etme fiili arasında "ve" bağlacı kullanılmaktayken 2016 yılında gelen yeni düzenlemede "veya" bağlacının

[414] Kayaer, "Bilişim Sistemine Girme", 101.; Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, (Ankara: Adalet Yayınevi, 2024), 1012-1015.
[415]Çakıcı, "M. 243 ve M. 244'te", 316.; Koca ve Üzülmez, *Özel Hükümler*, 1012-1015.
[416] Çakıcı, "M. 243 ve M. 244'te", 316.
[417] Melisa Lal, "Bilişim Sistemleri Aracılığıyla Haksız Yarar Sağlama Suçu", (Yüksek Lisans Tezi, Yaşar Üniversitesi, 2022): 9.; Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1030.; Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 995.
[418] İhtiyaroğlu, "Yargı Kararları Bağlamında", 427.
[419] Kayaer, "Bilişim Sistemine Girme", 97.; Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* 12/Özel Sayı (2010), 1395.
[420] Yüksektepe, *Soruşturma Usulü,* 442.
[421] İhtiyaroğlu, "Yargı Kararları Bağlamında", 409.
[422] Yüksektepe, *Soruşturma Usulü,* 442.
[423] İhtiyaroğlu, "Yargı Kararları Bağlamında", 410.

getirildiği görülmektedir[424]. Eski halde sisteme girdikten sonra orada kalmak suçun oluşması için şart iken ve AKSSS m. 2'de düzenlenen sisteme girmeyi yeterli gören hukuka aykırı erişim düzenlemesi ile uyumlu değilken[425], yeni halde suç bağlı hareketli suçtan seçimlik hareketli suça çevrilerek AKSSS ile uyum sağlanmaya çalışılmıştır[426]. Bu düzenlemeyle hem suçun oluşması için sisteme girilmiş olması yeterli hale gelmiş, hem de sisteme hukuka uygun bir şekilde girilmiş olsa bile, daha sonrasında, hukuka uygunluk ortadan kalktığı halde sistemden çıkılmaması durumu da suç olarak düzenlenmiş bulunmaktadır[427]. Düzenleme bu haliyle konut dokunulmazlığına benzer şekilde "elektronik konutun" ihlali niteliğindedir[428]. Bununla beraber, bilişim sistemlerinde saklanan kişisel veriler özel hayat açısından önem arz ettiğinden Anayasa m. 20'de yer alan "özel hayatın gizliliği" düzenlemesiyle; haberleşme ve iletişimin bilişim sistemleri ile yürütülmesi dikkate alındığında Anayasa m. 22'de düzenlenen "haberleşme hürriyeti" düzenlemesiyle bağlantılı bir düzenleme olduğu söylenebilmektedir[429].

Doktrinde maddede kullanılan sisteme "girmek" ibaresinin fiziki bir giriş izlenimi uyandırdığı ve bu sebeple çok da yerinde bir ifade olmadığı, İngilizcede "access" teriminin karşılığı "erişim" ifadesi olduğundan bu ifadenin kullanılmasının çok daha yerinde olacağı ifade edilmekte ve anılan madde mevcut haliyle kavram kullanımı noktasında eleştirilmektedir[430]. Doktrinde bir başka eleştiri de madde başlığının "bilişim sistemine girme" olarak düzenlenmiş olmasıyla yalnızca girme eyleminin cezalandırıldığı izlenimi vererek yanıltıcı bir görünüş oluşturması olup başlığın "girme ve kalma" şeklinde düzenlenmesinin daha yerinde olacağı ifade edilmiştir[431].

TCK m. 243'e yönelik önemli eleştirilerden biri de bilişim sistemlerine yönelik sisteme girme ve orada kalmaya devam etme eylemlerini önleme noktasında mevcut düzenlemenin tek başına yeterli olmadığı noktasındadır. Bu bağlamda, öğretide; Alman Ceza Kanunu m. 202c'de yer alan ve hazırlık hareketlerinin cezalandırılmasını öngören

[424] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 994.
[425] Erkan, "Bilişim Sistemine", 43.
[426] Dülger, *İnternet İletişim Hukuku,* 250.
[427] Dülger, *İnternet İletişim Hukuku*, 251.
[428] Akbulut, *Bilişim Alanında Suçlar*, 115.
[429] İhtiyaroğlu, "Yargı Kararları Bağlamında", 410.
[430] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 994. Karagülmez*, Bilişim Suçları,* 204.
[431] Erdoğan, "Kalma Suçu", 1368.

düzenlemelere benzer bir biçimde düzenleme yapılması ve TCK m. 243'te yer alan eylemlere yönelik hazırlık hareketlerinin de cezalandırılması gerektiği konusunda düşünceler mevcuttur[432]. Ancak kanaatimce, TCK m. 245/A'da yer alan düzenleme dikkate alındığında hazırlık hareketi olarak değerlendirilebilecek cihaz ve programların üretimi, dağıtımı ve bulundurulmasının suç olarak düzenlendiği dikkate alındığında, bu konuda büyük bir eksiklik oluşturmadığı da söylenebilir. Yine maddeye getirilen bir diğer eleştiri de; TCK m. 243/1'de geçen "sistemin bir kısmı" deyiminden ne anlaşılması gerektiği konusunda madde gerekçesinde açıklama getirilmediğinden, uygulamada sorunlar çıkabileceği ve bu durumun kanunilik ilkesini zedeleyebileceği noktasındadır[433]. Ancak bir bilişim sisteminin bütün parçalarının sistemin bizzat kendisini oluşturduğu ve bir bütün olarak kabul edilmesi gerektiği düşünülecek olursa; sisteme girmek tek başına suçun oluşmasına sebebiyet verecek olup sistemin hangi kısmına girildiği bu açıdan bir fark oluşturmayacağından, kanaatimce böyle bir düzenlemenin yapılmamış olması büyük bir eksiklik ifade etmemektedir. Doktrinde sistemin bir kısmına girmek ifadesiyle kastedilenin sisteme ait parçalardan herhangi birine girmek olduğu, bu bağlamda sisteme bağlı kullanılan CD ya da bellek gibi unsurlara da girmenin bu suça neden olacağı ve AKSSS kapsamında da benzer bir anlayışın mevcut olduğu ifade edilmiştir[434]. Doktrinde, sistemde kalmaya devam etmenin suçun tamamlayıcı unsuru olarak getirilmesinin kötü niyetli olmayıp kısa süreliğine giriş yapan, araştırma, yazılım başarısı test etme gibi amaçlarla sisteme giriş yapan kişilerin eylemlerini fazla katı bir düzenlemeyle suç saymama düşüncesinden kaynaklandığını, ancak bu halin suça teşebbüs olarak değerlendirilmesi gerektiği düşüncesinde olanlar vardır[435].

Gerekçede ve madde metninde sistemde kalmaya devam etme eyleminden ne anlaşılması gerektiği konusunda bir açıklık bulunmadığından doktrinde bu konuda farklı görüşler ortaya atılmıştır. Buna göre ilk görüş[436], her girme eyleminin kalma eylemini de içerdiğinden bahisle girme eylemi sonucu bir milisaniye de olsa kalmanın

[432] Dülger, *İnternet İletişim Hukuku*, 253.
[433] Demircan, *Bilişim Alanında Suçlar*, 66.
[434] Kayaer, "Bilişim Sistemine Girme", 101.
[435] Akarslan, *Bilişim Suçları*, 45.; Kurt, *Açıklamalı - İçtihatlı,* 148.
[436] Özbek, Doğan ve Bacaksız, Özel hükümler, 995.; Soyaslan, *Özel Hükümler*, 637. Recep Yılmaz Yazıcıoğlu, "Hukukumuzda TCK'nun 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi", İçinde Bilişim Hukuku Konferansı, (Ankara: Yargıtay Başkanlığı Yayını, 2009), 83.

gerçekleştiğini ifade ederken; ikinci görüş[437], kişinin sisteme girdiğini anlamasına rağmen sistemde kalmaya devam etmesi halinde suçun oluştuğunu, suç ile korunan hukuki değerleri ihlal edecek düzeyde bir kalmanın suçun oluşumu için yeterli görüleceğini ifade etmektedir[438]. Söz konusu görüşler de değerlendirildiğinde somut olayda süre yönünden madde metninde bir bağlayıcılığın olmaması suçun fiil ve yöntem açısından tartışılmasını ve sisteme girilip girilmediği ile sistemde kalmaya devam edilip edilmediğinin değerlendirilmesini gerektirmektedir[439]. Bununla birlikte kalma eyleminin ne kadar süre gerçekleştiğinin cezanın belirlenmesi noktasında da önemli olduğu ifade edilmektedir[440].

Maddenin devamında TCK m. 243/2'de daha az ceza verilmesini öngören nitelikli hal düzenlenmiş, sisteme girme veya sistemde kalma fiillerinin bedeli karşılığı yararlanabilen sistemler hakkında işlenmesi hali indirim sebebi olarak görülmüştür. Bu düzenlemenin temel sebebi bedeli karşılığı yararlanılan sistemlerde diğer sistemlere nazaran mahremiyetin daha az görülmesidir[441]. TCK m. 243/3'te ise fiil nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi durumu suçun neticesi sebebiyle ağırlaşmış hali olarak düzenlenmiştir[442].

TCK m. 243/4'te "*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*." denilmek suretiyle farklı bir suç tipi düzenlendiği görülmektedir. AKSSS'de yer alan yasadışı araya girme başlıklı m. 3 ile uyum sağlamaya yönelik çıkarılan düzenlemenin gerekçesinde; yasadışı araya girme fiillerinin bilişim sistemine girilmeksizin, teknik araçlarla gerçekleştirilen eylemlerden olduğu ve bütün elektronik veri transferlerinin korunması amaçlanan gizlilik kapsamında kaldığı belirtilmiştir[443]. Doktrinde bu düzenlemenin bu konudaki

[437]Pallı, "Hukukta Bilişim Suçları", 157.; Hakan Karakehya, "Türk Ceza Kanununda Bilişim Sistemine Girme Suçu", *Türkiye Barolar Birliği Dergisi*, 81 (2009), 14.; Kurt, *Açıklamalı - İçtihatlı,* 154.; Kubilay Taşdemir, *Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları*, (Ankara: Ütopyagrafik, 2009), 259.; Osman Yaşar, Hasan Tahsin Gökcan ve Mustafa Artuç, *Yorumlu – Uygulamalı Türk Ceza Kanunu*, (Ankara: Adalet Yayınevi, 2014), 7292.
[438] Detaylı bilgi için bkz: Erdoğan, "Kalma Suçu", 1377.
[439] İhtiyaroğlu, "Yargı Kararları Bağlamında", 426.
[440] Kayaer, "Bilişim Sistemine Girme", 104.; Özbek, Doğan ve Bacaksız, Özel hükümler, 995.
[441] Erkan, "Bilişim Sistemine", 151.
[442] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 995.
[443] Akbulut, *Bilişim Alanında Suçlar*, 157.

eksikliği karşılama noktasında son derece yerinde olduğu[444], ancak düzenlemenin madde başlığı ile örtüşmediği[445] ve TCK m. 243/4 yerine ayrı bir başlık altında düzenlenmesinin daha yerinde olacağı noktasında eleştirilmektedir[446].

Bilişim sistemine girme suçu doktrinde bir görüşe göre, sisteme girilmesini zorunlu kılan başka bilişim suçlarının işlenmesinde araç suç konumunda bulunduğundan, gerçekleştirilmesi hedeflenen suç bakımından geçit olma özelliği taşımakta iken[447]; diğer bir görüşe göre, örneğin hukuka uygun bir biçimde sisteme giren failin sisteme girdikten sonra zarar verici eylemde bulunmasında olduğu gibi, sisteme hukuka aykırı girmek noktasında mutlak bir mecburiyet bulunmamakta, korunan hukuki değerlerin farklılığı da gözetildiğinde geçitli suç söz konusu olmamaktadır[448]. Yargıtay'ın da bu konuda vermiş olduğu 2014 tarihli bir kararda; *"...katılanın facebook hesabına giriş için kullandığı elektronik posta adresini, rızası dışında ele geçiren sanık hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesinde bir isabetsizlik görülmemiş..."*, "*...bilişim sistemindeki katılana özel kısma girip, hukuka aykırı olarak sistemde kalmaya devam eden ve katılanın bilişim sistemindeki kendisine ait kısma erişimini engelleyen sanık hakkında, TCK'nın 244/2. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan ayrıca mahkumiyet kararı verilmesi gerektiğinin gözetilmemesi...*"[449] denilmek suretiyle her iki suç tipinin de ihlal edildiği ve her iki suç tip içinde mahkumiyet kararı verilmesi gerektiği ifade edilmiştir[450].

1.5.5.2. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244)

TCK m. 244/1'de bilişim sisteminin işleyişini engellemek, bozmak; TCK m. 244/2'de bir bilişim sistemi içindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek suç olarak

[444] Dülger, *İnternet İletişim Hukuku*, 326.
[445] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 996.
[446] Akbulut, *Bilişim Alanında Suçlar*, 158.
[447] Yavuz Erdoğan, "Kalma Suçu", 1418.
[448] Dülger, *İnternet İletişim Hukuku*, 319.; Aköz, "Mevzuat Önerileri", 99.
[449] Yargıtay 12. Ceza Dairesi, 15.09.2014, E. 2014/649, K. 2014/17770, https://kararara ma.yargitay.gov.tr/, E.T. 15.01.2025.
[450] Aköz, "Mevzuat Önerileri", 99.

düzenlenmiştir. 1. fıkrada düzenlenen suç bir bilişim sistemine yönelik eylemlerden oluşurken, 2. fıkrada düzenlenen suç sistemdeki verilere yönelik eylemlerden oluşmaktadır. TCK m. 244/1-2'de yer alan bu düzenlemeler ile AKSSS m. 4. ve 5.'te yer alan sisteme etki etme ve verilere etki etme düzenlemelerine uyumluluk sağlanmaya çalışıldığı görülmektedir[451].

TCK m. 244/3'te eylemlerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali nitelikli hal olarak düzenlenmiş olup, TCK m. 244/4'te ise tanımlanan fiillerin işlenmesi ile kişinin kendisi veya başkası yararına haksız bir çıkar sağlaması başka bir suç oluşturmuyor ise bir görüşe göre ayrı ve bağımsız bir suç diğer bir görüşe göre ise nitelikli hal olarak düzenlenmiştir.

TCK m. 244'ün gerekçesinde ise bilişim sisteminin fiziki varlığı ve işlemesini sağlayan tüm diğer unsurlarının bu suçun konusunu oluşturduğu ifade edilmiş, böylece sistem maddi ve soyut tüm unsurları ile koruma altına alınmaya çalışılmıştır[452]. TCK m. 244'e ikinci bölümde detaylıca yer verilecektir.

1.5.5.3. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)

TCK m. 245'in ilk üç fıkrasında; "*Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır*.

Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı

[451]Dülger, *İnternet İletişim Hukuku*, 334.; Yavuz Erdoğan, *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, (İstanbul: Legal Yayıncılık, 2012), 180, 211. Yazıcıoğlu, "Yeni Türk", 117.
[452] Dülger, *İnternet İletişim Hukuku*, 335.

gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır." denilmek suretiyle üç farklı suç tipi düzenlenmiş olup, ilk fıkrada gerçek bir kartın kullanılarak hukuka aykırı yarar sağlanması, ikinci fıkrada sahte kart üretme, üçüncü fıkrada ise sahte kart kullanarak hukuka aykırı yarar sağlama fiilleri suç olarak düzenlenmiştir[453].

765 sayılı eski TCK'da banka ve kredi kartlarının kötüye kullanılmasıyla ilgili bir düzenleme bulunmadığından bu tarz eylemler hem doktrinde hem yargıda karmaşaya yol açmakta ve Yargıtay'a göre kimi zaman aynı kanunun 525/b-2 maddesi kapsamında, kimi zaman da hırsızlık veya dolandırıcılık olarak değerlendirilmekteydi[454]. Banka ve kredi kartlarının kötüye kullanılması olaylarının hangi suç tipi kapsamında görülmesi gerektiği yalnızca Türk hukukunda değil, aynı zamanda diğer hukuk sistemlerinde de tartışılan konulardan biri olmuş, mevzuatlarda bu konuda düzenlemeye gidilene kadar bu karışıklık devam etmiştir[455]. Sonuç olarak 5237 sayılı TCK'da bu suçlar ayrı bir başlık altında düzenlenerek tartışmalara son verilmek istenmiş ve madde gerekçesinde de belirtildiği üzere banka ve kart sahiplerinin zarara sokularak haksız çıkar sağlanmasının önüne geçilmek istenmiştir[456]. Ancak başlangıçta iki fıkra olarak ortaya çıkan TCK m. 245, ilk düzenlenmesinden sonra da defalarca kez değişikliğe uğramış ve sırasıyla 2, 4 ve 5. fıkralar eklenerek en çok değişikliğe gidilen hükümlerden biri olmuştur[457].

Madde gerekçesinde "*bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak*" ve yaşanan içtihat karmaşasını önlemek maddenin çıkarılış amacı olarak gösterilmiş ve doktrinde bu gerekçeyle daha çok malvarlığına yönelik suç izlenimi oluşturduğu ifade edilmekle beraber, düzenlenme yeri ile asıl koruduğu değerin bilişim alanı ve güvenliği olduğu, bu sebeple koruduğu hukuki yararın karma bir nitelik arz ettiği belirtilmiştir[458]. Doktrinde yer alan bir başka görüşte ise bu suçla korunmak istenen değerin hırsızlık, dolandırıcılık, güveni kötüye

[453] Dülger, *İnternet İletişim Hukuku,* 382.
[454] Akbulut, *Bilişim Alanında Suçlar*, 270.
[455]Detaylı bilgi için bkz: Akbulut, *Bilişim Alanında Suçlar*, 270 vd.
[456] Dülger, *İnternet İletişim Hukuku,* 383.; Yazıcıoğlu, "Yeni Türk", 119.
[457] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1021.
[458] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1023.

kullanma suçlarını içerdiğinden malvarlığı ve kişilere duyulan güven; sahtecilik suçunu içerdiği için de kamuya duyulan güven ve itibar olduğu ifade edilmektedir[459].

Suçun faili sahte banka kartı üreten kimse olabileceği gibi bunun dışındaki üçüncü bir kişi de olabilir, ancak; failin kartın mahiyeti konusunda bilgi sahibi olması gereklidir[460]. Suçun mağduru ise herkes olabilir.

TCK m. 245'i suçun oluşması noktasında incelersek; TCK m. 245/1'deki suçun oluşmasında kartın ele geçirilmesi yeterli olmayıp kartın kullanılmasına yönelik davranışlarda bulunulması gerekmekte ise de kartı kullanmaya yönelik davranışlar gerçekleştirilmişse ve kart kullanıldığı halde yarar sağlanamamışsa suç teşebbüs aşamasına ulaşmış olacaktır[461]. Kartın ne şekilde kullanılacağına ilişkin ise bir belirleme yapılmadığından ATM'den para çekme veya alışveriş sırasında kullanılması bu noktada mümkündür[462]. Kanun maddesinde kartın her ne suretle olursa olsun ele geçirilmesi ifadesi kullanıldığından, eylemin geniş olarak düşünülmesi gerekecek ve sadece hukuka aykırı elde edinimler değil, rıza dahilinde ya da görev gereği kartın elde bulundurulması halinde de bu suç işlenebilecektir[463]. Banka kartının hukuka aykırı yollarla ele geçirilmesi halinde ise, Yargıtay Ceza Genel Kurulu 2010 tarihli bir kararında; "…*5237 sayılı TCY'nin 245/1. maddesindeki banka veya kredi kartlarını kötüye kullanma suçu bileşik suç olarak düzenlenmemiş olup, yasa maddesinde geçen ""her ne surette olursa olsun" ifadesi banka veya kredi kartlarının sadece hukuka uygun yollardan ele geçirilmesini kapsamaktadır. Bunun sonucu olarak; sanığın kurduğu düzenek ile ATM makinesine para çekmek için gelen mağdurların şifresini de öğrenmek suretiyle ele geçirdiği, ekonomik değeri bulunduğunda kuşku bulunmayan menkul mal niteliğindeki banka kartı ile başka bir ATM cihazına gidip para çekmesi şeklinde gerçekleştirdiği eylemlerinde, banka veya kredi kartının kötüye kullanılması suçu yanında hırsızlık suçu da oluşmaktadır.*"[464] denilmek suretiyle TCK m. 245'de yer alan suçun kartın ele

[459] Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", *Journal of İstanbul University Law Faculty*, 71/1 (2013): 871.
[460] Mahmutoğlu, " Yargı Kararları Işığında", 871.
[461] Yüksektepe, *Soruşturma Usulü,* 480.
[462] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1032.
[463] Yılmaz ve Güllüpınar, "Kriminolojik Açıdan", 5391.
[464] Yargıtay Ceza Genel Kurulu, 30.03.2010, E. 2010/11-17, K. 2010/65, https://kararara ma.yargitay.gov.tr/, E.T. 15.01.2025; Metin Turan ve Özgür Külcü, "Türkiye'de Bilişim

geçirilmesi eylemini kapsamadığını, ayrıca kartın ele geçirilmesi bakımından hırsızlık suçundan hüküm kurulması gerektiğini belirtmiştir. TCK m. 245/2'deki suçun oluşması için ise sahte kart üretim faaliyetinin doğrudan fail tarafından gerçekleştirilmesi gerekmemekte, sahte belgelerle başvurarak bankaya kart düzenletmesi de failin cezalandırılması için yeterli görülmekte (öğretide sahte belgeyle başvuru sonucu bankadan alınan kartın TCK m. 245/2-3 anlamında sahte kart olmadığına yönelik görüşler[465] bulunmakla birlikte Yargıtay Ceza Genel Kurulu'nun bu konuda verdiği kararında[466] da sahte olduğu kabul edilmiştir), ancak hiçbir banka hesabıyla ilişkilendirilmeyen veya failin kendi hesabıyla ilişkilendirilen kartlar bu suçun oluşumuna sebebiyet vermemektedir[467]. TCK m. 245/3'teki suçun oluşabilmesi için ise sahte veya üzerinde sahtecilik yapılan kartın kullanılmış olması teşebbüs için yeterli olmakta, suçun tamamlanması için ise haksız çıkar sağlanması gerekmektedir[468].

TCK m. 245/4'te gerçek bir kartın kullanılarak hukuka aykırı yarar sağlanması eyleminin haklarında ayrılık kararı verilmemiş eşlerden birinin, üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın veyahut aynı konutta beraber yaşayan kardeşlerden birinin zararına işlenmesi durumu bir şahsi cezasızlık nedeni[469] olarak görülmüş; TCK m. 245/5'te ise TCK m. 245/1'e ilişkin etkin pişmanlık hükümlerine yer verilmiştir[470].

TCK m. 245/1-2 bakımından mağdurun farklı kişi ya da kuruluşlar olması halinde ilk fıkra bakımından kart hamili, ikinci fıkra bakımından kuruluş sayısınca gerçek suç oluşur ve içtima uygulanmaz[471]. Nitekim Yargıtay 8. Ceza Dairesi'nin 2018 tarihli bir kararında[472] da banka sayısınca suçun oluşacağı ifade edilmiştir. Bununla birlikte aynı dairenin yine 2018 tarihli başka bir kararında da ifade edildiği üzere, aynı kişiye karşı

Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi", *Türk Kütüphaneciliği*, 28/1 (2014), 33.

[465] Soyaslan, *Özel Hükümler*, 665.

[466] Yargıtay Ceza Genel Kurulu, 27.05.2008, E. 2008/11-87, K. 2008/150, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.

[467] Yüksektepe, *Soruşturma Usulü*, 481.

[468] Yüksektepe, *Soruşturma Usulü*, 481.

[469] Doktrinde şahsi cezasızlık sebebi yerine şikâyete bağlı da düzenlenebileceği vurgusu yapılmıştır.: Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1034.

[470] Akbulut, *Bilişim Alanında Suçlar*, 275.

[471] Aköz, "Mevzuat Önerileri", 151.

[472] Yargıtay 8. Ceza Dairesi, 12.04.2018, E. 2017/22384, K. 2018/4133, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.

bu suçun farklı zamanlarda işlenmesi ayrı bir durum olup böyle bir durumda zincirleme suç hükümleri uygulanması gerekmektedir[473]. Suçun mağduru konusunda Yargıtay'ın vermiş olduğu bir karara göre; banka tarafından üretilen kredi kartının sahibine tesliminden önce ele geçirilerek hukuka aykırı olarak kullanılması gibi bir durumda suçun mağduru kart sahibi değil, banka olarak değerlendirilmektedir[474].

1.5.5.4. Yasak Cihaz ve Programların Bulundurulması ve Kullanılması Suçu (TCK m. 245/A)

2016'da 6698 sayılı KVKK m. 30'la getirilen TCK m. 245/A'da[475]; "*Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır*." denilmek suretiyle düzenlemeden önce eksikliği eleştirilen ve AKSSS'nin cihazların kötüye kullanımı başlıklı m. 6'da da öngörüldüğü üzere bilişim suçlarının işlenmesinde kullanılan cihaz ve programların üretilmesi, satılması, başkalarına verilmesi ve bulundurulması yasaklanmıştır[476]. Ancak TCK m. 245/A ile AKSSS m. 6 karşılaştırıldığında, AKSSS'de uygulanacak suçlar yasadışı erişim, araya girme, verilere ve sisteme müdahale ile sınırlanmışken TCK m. 245/A'daki düzenlemenin daha geniş bir belirleme yaptığı ve tüm bilişim suçlarını kapsar nitelikte olduğu görülmektedir[477]. Bu suç tipi ile bilişim suçlarında kullanılmak üzere üretilen program ve cihazların satıldığı karaborsanın büyümesinin önüne geçmek hedeflenmiştir[478].

---

[473]Yargıtay'ın zincirleme suç hükümleri uygulanmasına ilişkin kararı şu şekildedir: "*Şikayetçiye ait kredi kartını değişik zamanlarda birden çok kez kullanan sanık hakkında hüküm kurulurken TCK.nun 43. maddesinde düzenlenen zincirleme suç hükümlerinin uygulanmaması suretiyle eksik ceza tayini... gereğince bozulmasına...*"; Yargıtay 8. Ceza Dairesi, 16.06.2016, E. 2016/3862, K. 2016/8047, https://kararara ma.yargitay.gov.tr/, E.T. 15.01.2025.; Aköz, "Mevzuat Önerileri", 151.

[474]. Yargıtay 8. Ceza Dairesi, 18.01.2018, E. 2017/22781, K. 2018/560, https://kazanci.com.tr/, E.T. 15.01.2025.; Özsoy, "Doğrudan Bilişim Suçları", 322.

[475] Akbulut, *Bilişim Alanında Suçlar,* 344.

[476] Dülger, *İnternet İletişim Hukuku*, 501.

[477] Akbulut, *Bilişim Alanında Suçlar*, 346.

[478] Dülger, *İnternet İletişim Hukuku*, 503.

Doktrinde, kanun sistematiğinde madde başlıklarında suçun eylem unsuru ön plana çıkarılırken TCK m. 245/A için suçun konusunu oluşturan yasak cihaz ve programlar ifadesinin kullanıldığı, bununla beraber madde metninde bu cihaz ve programların yasak olduğuna ilişkin bir ifadenin yer almadığı, başlığın madde içeriğini yansıtmaktan uzak olduğu ve içerik çağrışımında bulunmadığı gerekçeleriyle başlık seçiminin eleştirildiği görülmektedir[479].

Madde gerekçesinde bilişim suçlarında kullanılmak üzere üretilen cihaz ve programların yasaklanarak bu suçlarla mücadelede etkinliği ve caydırıcılığı sağlamanın amaçlandığı belirtilmekte olup, suçun oluşumunda failin bu programlara ilişkin maddede sayılan eylemleri, örneğin; sistem güvenliğini test etmek amacıyla değil, suç işleme kastıyla gerçekleştirmesi gerekmektedir[480].

1.5.6. Yargı Kararlarında Bilişim Suçları

Türkiye'de bilişim alanında işlenen suçlardan Yargıtay'da temyiz incelemesinden geçenler dikkate alındığında, işlenen suçların büyük çoğunlukla doğrudan bilişim suçları olarak ifade ettiğimiz TCK m. 243-245 maddelerinin ihlali şeklinde gerçekleştirildiği görülmektedir[481]. Bu maddeler içerisinde Yargıtay kararlarında en çok karşılaşılan suçların ise TCK m. 245 ve TCK m. 244 olduğu görülmektedir[482].

Bilişim suçlarında uygulamada karşılaşılan sorunlarda; yerel mahkemelerin en çok suçun vasfını belirlemede hataya düştükleri, bu hataların bir kısmının 765 sayılı TCK ile 5237 sayılı TCK hükümlerinin karıştırılmasından ve getirilen hükümler arasındaki faklardan kaynaklandığı, nitelikli dolandırıcılık ile TCK m. 244/4 hükmünün niteliğinin belirlenmesinde problem yaşandığı, önceki kanun – sonraki kanun uygulama dönemlerine giren meselelerde lehe hükümlerin belirlenmesinde problem yaşandığı, ayrıca mahkemeler arası görevsizlik hususlarının da gerçekleştiği görülmüştür[483]. Tüm bunların sebepleri doktrinde kanun hükümlerinin yeterince açık olmaması, suçun vasfında hata, ilk defa karşılan hukuki problemler ve mevzuatın düzenlenmesi

[479] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1057.
[480] Akbulut, *Bilişim Alanında Suçlar*, 345.
[481] Turan ve Külcü, "İçerik Analizi", 44.
[482] Turan ve Külcü, "İçerik Analizi", 43.
[483] Turan ve Külcü, "İçerik Analizi", 44.

aşamasında hükümlerin ruhu ile lafzı arasında uygunsuzluk bulunması gibi durumlar gösterilmiştir[484].

1.5.7. Bilişim Suçlarının Klasik Suçlar Karşısındaki Konumu

Bireylerarası veyahut birey ile toplum arasındaki ilişkilerde etkili olan yeni gelişmelerin sonucunda, menfaatlerin ihlaline neden olan davranışlara karşı koruma sağlanması ihtiyacı, bu gelişmeleri bir kurala bağlama gereğini ortaya çıkarmaktadır[485]. Teknolojiyle toplumsal yaşamda meydana gelen değişiklikler, teknolojinin ortaya çıkardığı yaşam koşullarını iyileştirici etkilerin yanında, risk ve tehlikelerini taşımaktadır. Bu sebeple bilişim sistemlerinin kullanılmaya başlanması, bu sistemlere karşı ya da bu sistemler aracılığıyla işlenen ve toplum ya da bireylerin menfaatlerini ihlal eden eylemlere karşı koruma sağlanması ihtiyacını ortaya çıkarmıştır[486]. Bilişim alanında meydana gelen gelişim ve bu gelişimin toplum genelinde ulaşılabilir konuma gelmesi bilginin her kesimden insan tarafından ulaşılabilir olmasını sağlamış, bununla birlikte bilginin kişiler tarafından ne şekilde kullanılacağının kestirilememesi kontrol edilemeyen risklerin ortaya çıkmasına zemin hazırlamış ve Alman sosyolog Ulrich Beck'in ifadesiyle modern toplum aynı zamanda "risk toplumu" olarak görülmeye başlanmıştır[487]. Öğretide devlet ve toplum yapısındaki değişiklik ve gelişmelerin kanunkoyucunun faaliyetlerini doğrudan etkiler nitelikte bulunduğunu ve önceki düzenlemelerin eskiyerek kabul edilemez hale gelebileceği ifade edilmekle birlikte ceza hukukunun kendine özgü yapısı nedeniyle eskimeyi önlemenin çoğu zaman olanaklı olmadığı ifade edilmektedir[488].

Günümüz bilişim devrimi ile bilgi toplumu sisteminin ceza hukukundaki etkisi, klasik ceza hukuku anlayışının hukuksal değerleri koruma noktasında güvence fonksiyonunun zayıflaması olarak yansımıştır[489]. Klasik ceza hukukunun ulus devlet anlayışı egemenliğindeki dönemde şekillenmesi nedeniyle günümüz dünyasındaki küreselleşmenin gereklerini karşılayamaması, değişikliye uğramasını kaçınılmaz

[484] Turan ve Külcü, "İçerik Analizi", 44.
[485] Ersoy, "Hukuki Koruma Çerçevesinde", 153.
[486] Ersoy, "Hukuki Koruma Çerçevesinde", 153.
[487] İlker Tepe, "İnternet ve Ceza Hukuku – Modern Ceza Hukuku Teorisinde İnternet ve İnternet Suçluluğunun Konumu", *Ceza Hukuku Dergisi*, 4/9 (2009), 261.
[488] Yener Ünver, "İnternet Açısından", 57.
[489] Tepe, "İnternet Suçluluğunun Konumu", 263.

kılmıştır[490]. Modern ceza hukukunun ortaya çıkışında bilişim sistemleri ve bilgi toplumunun ortaya çıkışı etken olup bu konudaki değişimin ilk ekseni küreselleşmeyle birlikte sınır aşan suçların işlenmesi, ikinci ekseni ise bilgi toplumunda ortaya çıkan gelişmelerin suç yapılarında karmaşıklaşmaya yol açması olarak değerlendirilmekte ve klasik ceza hukuku bu karmaşayı çözmekte etkili görülmeyerek yapısal sınırlarının zorlanmasının bir sonucu olarak modern ceza hukukunun ortaya çıktığı görülmektedir[491]. Modern suç politikasında; klasik ceza hukuku politikasında suç olmaktan çıkarma eleştirel fonksiyonu getiren hukuksal değer koruma öğretisi değişiklik göstermiş ve suç haline getirme yükümlülüğü yükleyen tarzda yeni bir ödev katmıştır[492]. Bu yaklaşımın bir sonucu olarak doktrinde evrensel değerlerin tam netleştirilmemiş olması sonucu muğlaklığın ortaya çıkmasıyla; ceza hukukunun büyük ölçekte genişlediği ve soyut tehlike suçlarında artışa neden olduğu savunulmuş ve soyut tehlike suçları "modernitenin suç şekli" olarak ifade edilmiştir[493]. Doktrinde ayrıca AB hukukunda yalnızca ceza hukuku bağlamında değil, aynı zamanda diğer hukuk alanlarında da hukuksal değerlerin korunması noktasında bu tarz bir yükümlülük yüklendiği belirtilmektedir[494]. Ancak ceza hukuku bakımından suçlarla mücadelede, diğer hukuk alanları kadar genişlik bulunmamaktadır. Böyle bir durumda suç arz eden eylemlere karşı devletçe sınırsız müdahalede bulunulması, meşru müdafaa hakkının kullanıldığı anlamına gelmeyecek, hak ihlallerine neden olacaktır[495].

Modern ceza hukuku ile birlikte; kanuni düzenlemelerde yönelim zarar suçlarından tehlike suçlarına kayarak tehlike suçlarına endeksli bir gelişim süreci geliştirmiş, bunun bir sonucu olarak cezalandırılabilir alan genişlemiş ve hazırlık hareketlerinin de cezalandırılmasına yönelik düzenlemeleri beraberinde getirmiş, risk toplumu yapısı devletleri önleyici fonksiyonu öne çıkarmak adına "sola ratio" (ilk araç) olan normları kullanmaya itmiş ve belirlilik, kanunilik, kusur, şüpheden sanık yararlanır gibi temel

[490] Tepe, "İnternet Suçluluğunun Konumu", 266.
[491] Tepe, "İnternet Suçluluğunun Konumu", 264.
[492] Ünver, "İnternet Açısından", 54.
[493] Tepe, "İnternet Suçluluğunun Konumu", 265.
[494] Ünver, "İnternet Açısından", 55.
[495] Ünver, "İnternet Açısından", 58.

klasik ceza hukuku ilkelerinin uygulanmasında yumuşamalara ve istisnalarının artmasına yönelik eğilimler oluşturmuştur[496].

Teknolojinin gelişimi ve yaygınlaşması ile bağlantılı gelişim gösteren bilişim suçları modern ceza hukuku yönünde ortaya çıkan en önemli suçlardandır. Bilişim suçlarını diğer klasik suçlardan ayıran önemli birçok farklılıkları bulunmaktadır. Bilişim suçları globalleşmeyle beraber işlenme oranı devamlı artan, zaman ve mekândan bağımsız ve anlık gerçekleşen suçlar oldukları gibi dijital delil süreçleri içermesi nedeniyle de klasik suçlardan ayrılmakta[497] ve teknik bilgi gerektiren bir araştırma sürecini gerekli kılmaktadır. Bilişim suçları kolaylıkla tanımlanabilecek sınırlara sahip olmayan henüz neyin suç olup olmadığı konusunda net bir ayrımın olmadığı suçlardır[498]. Küresel boyutta işlenebilen yapısıyla birlikte bilişim suçlarında, klasik suçlarla mücadele yöntemleri yetersiz kalmakta ve uluslararası işbirliğinin etkin bir şekilde sağlanmasını gerektirmektedir. Yine failler açısından yüksek kazanç ve düşük yakalanma riski bulundurması da bilişim suçlarının klasik suçlardan ayıran önemli özelliklerindendir[499].

[496] Tepe, "İnternet Suçluluğunun Konumu", 266-268.
[497] Bkz: Akarslan, Bilişim Suçları, 38-40.
[498] Aytekin, Kılıç ve Çakır, "Siber Suçlar", 182.; Hüseyin Çakır ve Ercan Sert, "Bilişim Suçları ve Delillendirme Süreci", İçinde *Örgütlü Suçlar ve Yeni Trendler*, ed. Oğuzhan Ömer Demir ve Murat Sever, (Ankara: Polis Akademisi Yayınları, 2011), 145.
[499] Bkz: Akarslan, Bilişim Suçları, 38-40.

İKİNCİ BÖLÜM

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

2.1.Genel olarak

Bilişim sistemlerine yönelik saldırılarda görülen artış ile bu saldırıların sıkça gündeme gelmeye başlamasıyla birlikte bu tür eylemler dikkat çekmiş ve mala zarar verme suçuna ilişkin düzenlemeler mal niteliğinde sayılmayan bilişim verilerine yönelik koruma sağlamadığından dolayı, bu tür soyut nitelikteki değerlerin korunması için düzenleme yapılması zorunluluğu ortaya çıkmıştır[500]. Bu konudaki düzenleme eksikliği AKSSS'den önce de birçok farklı devlet tarafından tespit edilmiş ve mevzuatlarda bu suçlara yönelik düzenlemelere yer verilmiştir[501]. Kanun koyucu da aynı şekilde bu eksikliği görerek TCK'da bir takım yeni düzenlemeler ortaya koymuştur. Bu düzenlemeler ile günümüzde sağlık, eğitim, sanayi, ulaşım, savunma gibi birçok alanda kullanılan ve işleyişinde kısa süreli aksamaların görülmesi halinde dahi üst düzeyde yıkıcı zararların ortaya çıkması tehlikesi bulunan bilişim sistemleri koruma altına alınarak, bu sistemlerin güvenliğine karşı gerçekleştirilecek eylemler cezalandırılmak istenmektedir. Bilişim sistemleri ve verilerin güvenliğinin sağlanması amacıyla kanun koyucunun ortaya koyduğu düzenlemelerden biri de sistemi engelleme, bozma, verileri yok etme ve değiştirmeye yönelik eylemlere karşı getirilen hükümlerdir. Ülkemizde bilişim sistemi ve veriye ilişkin ilk düzenleme 1991'de 765 sayılı TCK'ya 3756 sayılı

---

[500] Akbulut, *Bilişim Alanında Suçlar,* 176.

[501] Muammer Ketizmen, "Türk Ceza Hukuku'nda Bilişim Suçları", (Doktora Tezi, Ankara Üniversitesi, 2006), 139. Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, (Ankara: Adalet Yayınevi, 2008), 57.

kanunla getirilen m. 525/b-1'dir[502]. 5237 sayılı TCK'nın yürürlüğe girmesiyle ise 2005'te bu madde yürürlükten kalkmıştır. Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları 5237 sayılı TCK m. 244'de düzenlenmiş olup, madde metninde; "*Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

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

Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur." denilmek suretiyle bu suçlar yaptırım altına alınmıştır. Doktrinde bu suçların "bilgisayar ve içeriğini tahrip", "sistemi ve verileri tahrip[503]" ve "bilgileri otomatik işleme tabi tutan bir sisteme ve unsurlarına karşı nas'ı ızrar[504]" suçları olarak da adlandırıldığı görülmektedir[505].

TCK m. 244/1'de "sistemin işleyişini engelleme, bozma", TCK m. 244/2'de "sistemdeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, verileri başka yere gönderme" suç olarak düzenlenmiştir. Bu suçlar seçimlik hareketli olarak düzenlenmiş olup eylemlerden herhangi birinin gerçekleştirilmesi suçun oluşması açısından yeterlidir[506]. TCK m. 244/3'te "ilk iki fıkradaki eylemlerin banka veya kredi kurumuna ya da kamu kurum veya kuruluşuna ait sistemler üzerinde işlenmesi" bir ağırlaştırıcı hal olarak görülmüştür[507]. Başka suç oluşturmaması koşuluyla ilk iki fıkrada tanımlanan eylemlerin işlenmesi yoluyla haksız

[502] Ketizmen, "Bilişim Suçları", 141.
[503] Hatice Akıncı, A. Emre Alıç ve Cüneyd Er, "Türk Ceza Kanunu ve Bilişim Suçları", İçinde *İnternet ve Hukuk*, ed. Yeşim M. Atamer, (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004), 236.
[504] Yazıcıoğlu, *Bilgisayar Suçları*, 257.
[505] Demircan, *Bilişim Alanında Suçlar,* 83.
[506] Demircan, *Bilişim Alanında Suçlar,* 85.
[507] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1001.

çıkar sağlanması halini düzenleyen TCK m. 244/4 ise doktrinde tartışmalı olup; nitelikli hal mi yoksa ayrı bağımsız bir suç mu olduğu konusunda görüş ayrılıkları bulunmaktadır. TCK m. 244/4'te yer alan düzenleme TCK m. 244/1-2'nin nitelikli hali olduğu görüşüne katıldığımdan, bu konuya çalışmanın suça etki eden nedenler başlığı altında detaylı olarak yer verilecektir.

TCK m. 244, 765 sayılı Kanun döneminde hazırlanan 1997 ve 2003 tarihli TCK tasarıları esas alınmak suretiyle düzenlenmiştir[508]. TBMM Genel Kurulu'na sunulan tasarıda TCK m. 244'ün ilk iki fıkrası tek fıkra halinde düzenlenmiş ve her iki fıkrada yer alan tüm hareketler seçimlik hareket olarak tek suç tipi çatısında belirlenmişse de; genel kurulda kabul edilen önergede "*suç tanımlarında belirliliği sağlamak ve ceza miktarlarını işlenen fiillerin ağırlığına uygun olarak belirlemek*" gerekçesiyle ayrı iki fıkra haline getirilmiştir[509]. Bu değişiklikle, sistemin işleyişinin korunması verilerin korunmasına nazaran daha önemli görülerek ilk fıkraya ikinci fıkraya göre daha ağır bir yaptırım getirilmesi uygun bulunmuştur. Tasarılarda yer verilen para cezalarına, maddede yer alan suçlara teşebbüsün tamamlanmış suç gibi cezalandırılacağına dair belirlemeye ve 2. fıkra açısından hukuka aykırılığa işaret eden kavrama 5237 sayılı kanunda yer verilmemiş; tasarılarda bulunmayan 4. fıkrada eylemin başka suç oluşturmaması gerekliliğine ilişkin belirlemeye 5237 sayılı TCK'da tasarılardan farklı olarak yer verilmiştir[510].

TCK m. 244'ün 1. ve 2. fıkrası AKSSS m. 4.[511]'e ve 5.[512]'e uyum sağlamaya yönelik şekilde düzenlenmiştir. AKSSS m. 4'te veriye müdahale başlığı altında bilgisayar verilerinin tahribi, silinmesi, bozulması, değiştirilmesi ya da erişilmez hale

[508] Berrin Akbulut, "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi,* 24/2 (2016), 11.
[509] Dülger, *İnternet İletişim Hukuku*, 354.
[510] Akbulut, "Sistemi Engelleme", 12.
[511] AKSSS m. 4: *1. Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.*
2. Taraflardan biri, 1. Paragrafta tanımlanan fiillerin ciddi zararla sonuçlanması gerektiğini şart koşma hakkını saklı tutabilir.
[512] AKSSS m. 5:*Taraflardan her biri, bilgisayar sistemlerine veri girişi yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, değiştirerek veya engelleyerek bir bilgisayar sisteminin işleyişinin haksız yere engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.*

getirilmesine; AKSSS m. 5'te ise sisteme müdahale başlığı altında sisteme yeni veri yerleştirme, sistemdeki verileri başka yere gönderme, tahrip etme, silme, bozma, değiştirme yahut erişilmez hale getirmek suretiyle sistemin işleyişini ciddi bir şekilde engellemeye yönelik kasti eylemlerin suç olarak düzenlenmesi taraf devletlere yükümlülük olarak yüklenmiştir[513]. AKSSS m. 4'te verinin bir bilgisayar sistemi içerisinde ya da bir veri taşıyıcısında olması açısından bir ayrım gözetilmemiştir[514]. AKSSS m. 5'de yer alan eylemlerde ise sistemdeki verilere müdahale ya da sisteme veri gönderme gibi eylemlerle sistemin işleyişinin engellenmesi esas alınmış; sistemin fiziki olarak bir zarara uğraması aranmamış, donanıma ilişkin fiziksel müdahalelerse bu madde kapsamına alınmamıştır[515].

TCK m. 244 de ilk fıkrada AKSSS m. 5'e paralel bir biçimde bilişim sistemine yönelik fiiller düzenlenmişken, ikinci fıkrada AKSSS m. 4'e paralel bir biçimde sistemdeki verilere yönelik eylemler düzenlenmiş ve böylece iki ayrı fıkrada iki ayrı suç tipi oluşturulmuştur[516]. AKSSS'de yer alan düzenlemede verilere müdahalenin sisteme müdahaleden önce düzenlenmesinde özellikle bir sıra gözetildiği ve verilere müdahale edilerek sistemin işleyişine yapılan sistemi engelleme, bozma eylemlerinin de sisteme müdahale olarak görüldüğü gözlenmektedir[517]. TCK'da ise böyle bir sıra gözetilmemiştir. Yine sözleşmede her iki suç açısından da eylemlerin haksız gerçekleştirilmesi aranırken TCK'da böyle bir şart belirtilmemiştir[518]. Ayrıca sisteme veri yerleştirme, verileri başka yere gönderme eylemleri AKSSS'de m. 5'de düzenlenmişken TCK'da 2. fıkra kapsamına alınmıştır[519]. Yine AKSSS'de m. 4'de taraf devletlerin bu suçların oluşmasında ciddi zarar şartı arayabileceğini ifade etmiş olsa da[520] TCK bu suçların oluşumunda böyle bir kıstas getirmemiştir.

5237 sayılı TCK m. 244'ün gerekçesinde "*Sistemlere yöneltilen ızrar fiilleri özel bir suç haline getirilmiştir.*"[521] denilmek suretiyle sistemin çalışmasını engellemeye yönelik

[513] Convention on Cybercrime".
[514] Ketizmen, "Bilişim Suçları", 139.; Muammer Ketizmen, *Türk Ceza*, 51.
[515] Ketizmen, "Bilişim Suçları", 139.; Muammer Ketizmen, *Türk Ceza*, 51.
[516] Dülger, *İnternet İletişim Hukuku*, 334.
[517] Akbulut, *Bilişim Alanında Suçlar,* 177.
[518] Akbulut, *Bilişim Alanında Suçlar,* 177.
[519] Akbulut, *Bilişim Alanında Suçlar,* 177.
[520] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1001.; Ketizmen, "Bilişim Suçları", 57.; Muammer Ketizmen, *Türk Ceza*, 51.
[521] "Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu (1/593)", 156.

eylemler kastedilmekte[522], yine gerekçede mala zarar verme eylemlerinin bilişim araçlarına karşı işlenmesi halinin ayrı bir suç haline getirilerek özelleştirildiği ve sistemin "*fiziki varlığı ile işlemesini sağlayan tüm unsurlarını*"[523] kapsayacak şekilde topyekûn koruma altına alındığı ifade edilmektedir[524].

TCK m. 244/1 ve TCK m. 244/2'de yer alan suçların düzenlemesi 765 sayılı TCK döneminde m. 525/b'de yapılmış olup tek bir fıkrada düzenlenmişken, birtakım farklılıklarla birlikte bu suçların 5237 sayılı TCK'da iki ayrı fıkrada düzenlendikleri görülmektedir[525]. 765 sayılı TCK m. 525/b'ye göre; "*Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye……cezası verilir*." denilmek suretiyle bu suçların düzenlendiği görülmektedir. 765 sayılı TCK'ya göre 5237 sayılı TCK'da getirilen değişikliklere göre ise; "başkasına zarar verme, kendine veya başkasına yarar sağlama" amaçları aranmamış[526], bununla birlikte "sistemi erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme" eylemleri eklenmiştir. Böylelikle kişisel veri niteliğinde olmayan ve parasal değer taşımayan veriler de bu kapsamda koruma altına alınmıştır[527]. Ayrıca 765 sayılı TCK'da yer alan "tahrip etme" tabiri yeni TCK'da kullanılmamış[528], böylelikle AKSSS düzenlemesine de paralel bir biçimde sistemlerin donanımına mala zarar verme amacıyla gerçekleştirilen fiiller bu madde kapsamında değerlendirilmemiştir[529].

2.2. Suçla Korunan Hukuki Değer

TCK m. 244'de birden fazla suç tipi düzenlenmiş olması, bu suçla korunan hukuki değerin belirlenmesi noktasında da tartışmalara yol açmış ve öğretide birçok farklı görüşün ortaya atılmasına zemin hazırlamıştır. Bu tartışmalar 765 sayılı TCK

[522] Demircan, *Bilişim Alanında Suçlar,* 85.
[523] "Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu (1/593)", 156.
[524] Dülger, *İnternet İletişim Hukuku*, 335.
[525] Akbulut, *Bilişim Alanında Suçlar,* 173.
[526]Değirmenci, "2004 Türk", 205.
[527] Dülger, *İnternet İletişim Hukuku*, 335.
[528] Dülger, *İnternet İletişim Hukuku*, 335.
[529] Dülger, *İnternet İletişim Hukuku*, 335.; Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1002.

zamanında başlamış ve bu suçların düzenlendiği m. 525/b-1 üzerinden birçok farklı değerlendirme ve yaklaşım oluşturulmuştur[530].

765 sayılı TCK zamanında bu suçun "mala zarar verme" suçu ile ilgisine dikkat çekilerek değerlendirme yapıldığı görülmektedir[531]. 765 sayılı TCK hem sisteme ve sistemin soyut unsurlarına zarar verici eylemleri, hem de sistemin işleyişine engel olma ya da yanlış işlemesini sağlama eylemlerini tek hüküm olarak düzenleyerek bu tartışmaların alevlenmesine neden olmuştur[532]. Öğretide yer alan görüşlerden birinde göre bu suç klasik mala zarar verme suçunun özel bir şekli olup korunan hukuki değer mülkiyet hakkıdır[533]. Bu görüşe göre; sistem kullanıcısının sistemin düzgün çalışmasındaki menfaati ve ekonomik haklar da koruma altına alınmakta ve sistemin hem fiziki hem soyut elemanlarını kapsayan bir koruma sağlanmaktadır[534]. Başka bir görüşe göre bu suçlar ekonomik suç kategorisinde olup kanunkoyucu özel kast belirtmek suretiyle bu niteliği vurgulamaktadır. Ancak burada korunan hukuki değer kamu ekonomisi değil, bireysel malvarlığı olup hükümde kamu ekonomisinin korunduğuna dair bir unsur bulunmamaktadır[535]. Başka bir görüşe göre de düzenlemeyle sistemin arızasız çalışmasındaki fayda ve verilerin engelsiz kullanımı korunmakta olup, sistemin fiziki yapısına yönelik eylemlerin yaptırıma bağlanmasının amacı sistemin arızasız çalışmasıdır[536]. Bu görüşe karşı olanlarsa sistemin fiziksel kısmına yönelik eylemlerin değil yalnızca sistemin elektro-manyetik alanına; yani sistemin yazılımına yönelik eylemlerin cezalandırılmasının amaçlandığını, bu şekilde program ve verilerin çalışmasının korunduğunu savunmuşlardır[537].

5237 sayılı TCK dönemine gelindiğinde ise suçla korunan hukuki değer konusunda eski TCK'ya göre farklı değerlendirmeler yapıldığı görülmektedir. Eski TCK'da yapılan sisteme zarar vermeye yönelik düzenlemeye yeni TCK'da yer verilmemesi de bu durumu etkileyen sebeplerden biri olmuştur[538]. Ayrıca 765 sayılı kanunda tek bir bütün

[530] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1002.
[531] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1002.
[532] Akbulut, *Bilişim Alanında Suçlar*, 178.
[533] Yazıcıoğlu, *Bilgisayar Suçları*, 258.
[534] Yazıcıoğlu, *Bilgisayar Suçları*, 260.
[535] Ersoy, "Hukuki Koruma Çerçevesinde", 166.
[536] Akbulut, *Bilişim Alanında Suçlar*, 179.
[537] Ersoy, "Hukuki Koruma Çerçevesinde", 177.
[538] Akbulut, *Bilişim Alanında Suçlar*, 180.

şeklinde düzenlenen sisteme yönelik eylemlerle verilere yönelik eylemlerin, 5237 sayılı kanunda farklı fıkralarda düzenlenmiş olması bazı yazarlar tarafından her fıkra açısından farklı hukuki yarar tespit edilmesinde etkili olmuştur.

Her iki fıkra için ayrı belirleme yapan görüşe göre; ilk fıkrada sistem sahipleri, sistem işletmecileri ile kullanıcılarının sistemin usulünce çalışmasındaki yaralarının korunduğunu, ikinci fıkrada ise veri ve programlara karşı kasti zarar verme eylemlerine karşı korumanın sağlanmaya çalışıldığı ve verilerin kullanımındaki yararın korunduğu ifade edilmektedir[539]. Doktrinde bazı yazarlar ilk fıkrada sistem sahibinin mülkiyet hakkının[540] da korunduğu, bununla birlikte mülkiyet hakkı bulunmayan kullanıcıların da sistemin dokunulmazlığı, iletişim kurma, teknolojik gelişim özgürlüğü gibi haklarının korunduğunu savunmaktadır[541]. İkinci fıkrada ise bazı durumlarda mülkiyet hakkının ihlal edildiği, bazı durumlarda ise, örneğin; bir sanatçının eserini barındıran veriler açısından değerlendirildiğinde, fikri mülkiyet hakkının ihlal edilebileceği ifade edilmektedir[542]. Mülkiyet hakkının korunduğu düşüncesine karşı olanlar ise sistemin malik olmayan kullanıcılar tarafından kullanılması halinde de bu suçların oluşması ve malik olmayan kullanıcıların da korunmasını göz önüne alarak, burada mülkiyetin korunduğu düşüncesini reddetmektedir[543]. Başka bir görüşe göre ise bu suçlarda her ne kadar bireysel malvarlığı değeri ihlal edilse de kanun sistematiğinde düzenlendiği yer dikkate alındığında, bireyin malvarlığına dâhil bir değerden ziyade, bilişim sistemlerin düzgün şekilde işleyişi korunmaktadır[544].

TCK m. 244'te düzenlenen suçları mala zarar verme suçunun özel bir şekli olarak gören görüşe göre; bu suçun düzenlenmesinde bilişim sistemlerinin içerisinde yer alan yazılımsal süjelere yönelik eylemlerin klasik mala zarar verme suçu olarak görülüp görülemeyeceği konusundaki tartışmalara son vermenin amaçlandığı ve burada korunan hukuki değerin klasik mala zarar verme suçuna paralellik gösterdiği ifade

[539]Akbulut, *Bilişim Alanında Suçlar*, 181.
[540] Eker, "Eski TCK Bağlamında", 124.
[541]Kurt, *Açıklamalı - İçtihatlı,* 162.; Demircan, *Bilişim Alanında Suçlar,* 86.; Ömer Demirci, *Bilişim Suçları ve Soruşturma Yöntemleri*, (Ankara: Seçkin Yayınları, 2022), 94.; Ali Parlar, *Türk Ceza Hukukunda Bilişim Suçları*, (Ankara: Sage Yayıncılık, 2014), 37.
[542] Kurt, *Açıklamalı - İçtihatlı,* 162.; Demircan, *Bilişim Alanında Suçlar,* 86.; Ali Parlar, *Türk Ceza,* 37.
[543] Akbulut, *Bilişim Alanında Suçlar*, 182.; Akbulut, "Sistemi Engelleme,", 19.
[544] Koca ve Üzülmez, *Özel Hükümler*, 1025.

edilmektedir[545]. Bu görüşte, bilişim sistemi ve içerisinde yer alan verilerin mala zarar verme suçunun konusu olan mal tabiri kapsamına girmemesi sebebiyle oluşan boşluğu doldurmak amacıyla böyle bir düzenleme yapıldığı ifade edilmektedir[546]. Bu görüşe göre söz konusu suçta yer alan eylemlerin mala zarar verme kapsamındaki eylemler olduğu ve bu kapsamda malvarlığının korunmasının amaçlandığı savunulmaktadır[547]. Yine bu görüşe katılanlardan bazıları malvarlığının yanında ayrıca sisteme olan güvenin de korunduğunu ifade etmektedirler[548]. Buna göre bilişim sistemlerine karşı gerçekleştirilecek saldırılar dolayısıyla malvarlığı yönünden bir zarar ortaya çıkacağı gibi, toplumca bilişim sistemlerine duyulan güven de zedelenecek ve bu durum ekonomik düzeni de zarara uğratacaktır[549]. Mülkiyet hakkının korunduğunu ileri süren görüşte, özellikle TCK m. 244/4'te yer alan hükmün haksız menfaat teminini içermesi malvarlığı haklarının korunduğuna yönelik önemli bir argüman olarak kullanılmıştır[550].

Doktrinde yer alan başka bir görüşte, TCK m. 244'te yer alan suçların "Topluma Karşı Suçlar" kısmında düzenlenmiş olması da göz önünde bulundurularak, bu suçlarla korunan hukuki değerin bilişim sistemlerinin bütünlüğü ve güvenliği ile toplum çıkarları olduğu[551], bununla birlikte; özelikle bilişim sistemleri konusunda yeterli donanımı olmayan kişilerin güveninin korunmasına yönelik bir düzenleme olduğu da savunulmuştur[552].

Karma görüşü benimseyenler, burada hem mülkiyet hakkının hem de bilişim sistemi ve verilerin çalışabilirliğinin korunduğunu ifade etmektedir. Bu görüşe göre verilerin tamamı bir bilişim sisteminin unsuru niteliğinde olmayıp bir kısmı sistem içerisinde tek başına mevcut olan unsurlar olduğundan, TCK m. 244'te her iki fıkra birlikte değerlendirildiğinde hem sistemin hem de verilerin sağlam ve güvenli bir biçimde

[545] Ketizmen, "Bilişim Suçları", 152.; Muammer Ketizmen, *Türk Ceza*, 128.
[546] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1044.; Ketizmen, "Bilişim Suçları", 152.
[547] Ketizmen, "Bilişim Suçları", 152.; Muammer Ketizmen, *Türk Ceza*, 128.
[548] Gül, *Doğrudan Dolaylı*, 131.; Hasan Gerçeker, *Yorumlu ve Uygulamalı Türk Ceza Kanunu*, (Ankara: Seçkin Yayıncılık, 2022), 2207. Yaşar, Gökcan ve Artuç, *Yorumlu – Uygulamalı*, 7307.
[549] Apaydın, *Bilişim Ceza Hukuku*, 157.; Ali Parlar, *Türk Ceza*, 37.
[550] Mehmet Can Karagöz, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)", (Yüksek Lisans Tezi, Akdeniz Üniversitesi, 2019), 111.; Özbek, Doğan ve Bacaksız, Özel Hükümler, 1004.
[551] Karagöz, "Bilişim Sistemini", 112.; İrem Geçmez, *Bilişim Sistemini Engelleme, Bozma Verileri Yok Etme veya Değiştirme Suçları (TCK M. 244)*, (Ankara: Seçkin Yayınları, 2020), 79.; Erdoğan, "Engelleme Bozma", 146.
[552] Erdoğan, "Engelleme Bozma", 191.; Karagöz, "Bilişim Sistemini", 112.

çalışabilirliği korunmaktadır[553]. Buna göre bir bilişim sisteminde yalnızca veri veya yazılımlardan oluşan kısım koruma altına alınmakla kalmayıp, aynı zamanda donanım kısmı da koruma kapsamına dâhil edilmektedir[554]. Düzenlenen eylemlerin sistem ve veri sahibinin tasarruf yetkisine açık bir tecavüz niteliği taşıyan eylemler olmaları ve TCK m. 244/4'te haksız menfaat elde etmeye yönelik düzenlemenin mevcut olması birlikte değerlendirildiğinde burada mülkiyet hakkının da koruma altına alındığı ifade edilmektedir[555]. Ancak karma görüşü benimseyenlerden; failin eyleminin her iki suç tipini de ihlal edici nitelikte olması halinde kastın ortaya çıkarılabilmesi için bu suçlarla korunan hukuki değerlerin birbirinden ayrı olarak belirlenmesi gerektiğini düşünenler de mevcuttur[556]. Buna göre; ilk fıkrada yalnızca sistemden bahsedilmesi dolayısıyla sistemin kesintisiz ve düzgün bir şekilde çalışmasının korunduğu, ikinci fıkrada ise sistemde bulunan ancak sistemin işleyişini etkilemeyecek nitelikteki verilerin korunduğu ifade edilmektedir[557]. Sisteme zarar verilmesiyle de içerdiği verilere ulaşma veya içerdiği verilerin zarar görme ihtimalinin yüksek olması sebebiyle birinci fıkrada ikinci fıkraya nazaran daha ağır bir yaptırım düzenlendiği ifade edilmektedir[558]. Yargıtay 11. Ceza Dairesi'nin bir kararında ise *"...Bilişim sistemlerinin veya verilerin zarar görmesi halinde, kişinin malvarlığında bir azalma meydana geleceği gibi toplumun, bilişim sistemlerinin işleyişine olan güvenleri ve ekonomik düzenin sağlıklı işleyişi etkilendiği, bilişim sistemlerinin zarar görmeden işler durumda bulunmasında toplumsal yarar olduğu için yasanın "topluma karşı işlenen suçlar" kısmına alınmıştır.*" denilmek suretiyle birden fazla hukuki değerin korunduğu ifade edilmiştir[559]. Bu konuda diğer bir düşünce şekline göre ise bu suçlarda dar ve geniş anlamda olmak üzere iki farklı korunan hukuki değer bulunmaktadır. Buna göre bir görüşe göre dar anlamda mülkiyet hakkı korunmaktayken, geniş anlamda bilişim sistemlerinin bütünlüğü ve güvenliği korunmaktadır[560]. Diğer bir görüş ise dar anlamda bilişim sisteminin işleyiş ve güvenliği ile mülkiyet ve iletişim haklarının; geniş anlamda ise ülke ekonomisi ile

[553] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1001.; Dülger, İnternet İletişim Hukuku, 335.
[554] Dülger, *İnternet İletişim Hukuku*, 335.
[555] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1004.
[556] Dülger, *İnternet İletişim Hukuku*, 336.
[557] Dülger, *İnternet İletişim Hukuku*, 337.
[558] Dülger, *İnternet İletişim Hukuku*, 336.
[559] 11. Ceza Dairesi, 07.10.2009, E. 2009/1616, K. 2009/11328, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.
[560] Karagöz, "Bilişim Sistemini", 113.

kamu düzeni ve güvenliğinin korunduğunu ifade etmektedir[561]. Yine bu görüşte olanlardan bazıları; her ne kadar madde gerekçesinde bu suçların mala zarar vermenin özel bir şekli olduğu ifade edilmişse de günümüzde ağlarla birbirine bağlı birçok bilişim sistemi ve bilişim sistemi hizmetinin varlığı ve birine yapılan saldırının diğerlerine açık tehdit oluşturduğu düşünüldüğünde, bu suçlarla kamu güvenliğinden kamu düzenine kadar bu alanın tamamının korunmak istendiğini ve yine bu kapsamda; 3. fıkrada yer alan nitelikli halin toplumun tamamının mağduriyetini doğuracağından hareketle getirildiğini ve aslında bu nitelikli halin toplumun tamamının korunmak istendiğinin başka bir göstergesi olduğunu ifade etmektedir[562].

Doktrinde yer alan bir diğer görüş ise Bilişim Alanında Suçlar'ın Topluma Karşı Suçlar bölümünde düzenlenmesinin doğru olmadığını, burada yer alan suçların tamamının gerçek ya da tüzel kişilere karşı işlendiğini, Kişilere Karşı Suçlar bölümünde düzenlenmesinin daha yerinde olacağını ifade etmiştir[563]. Bu görüşe göre bu suçlarla sistem ile veriler üzerinde tasarruf yetkisi sahibi kişinin, verilerin içerdiği yazılım, bilimsel çalışma, ekonomik bilgi ve benzeri değerlere engelsiz ve arızasız ulaşmasındaki fayda korunmaktadır[564].

Suçla korunan hukuki değer konusunda gerek madde gerekçesi gerekse doktrinde bu konuda yer alan görüşler birlikte değerlendirildiğinde; hem 765 sayılı TCK'da hem de 5237 sayılı TCK'da, sisteme müdahale ve veriye müdahale suçları açısından, mülkiyet hakkının korunduğunu ifade eden görüşün baskın kabul gördüğü söylenebilmektedir[565]. Bu dahilde bir görüşe göre TCK m. 244'te yer alan suçların mala zarar verme suçunun özel bir şekli olduğu ifade edilmekle birlikte, kanun sistematiği açısından aynı amaca hizmet eden bu suçların aynı bölümde düzenlenmemesi ve bununla birlikte mala zarar verme suçunda yararlanılabilen şahsi cezasızlık sebepleri ile etkin pişmanlık hükümlerinin TCK m. 244'te yer alan suçlar açısından geçerli olmaması eleştirilmekte ve bir eksiklik olarak değerlendirilmektedir[566].

[561] Apaydın, *Bilişim Ceza Hukuku*, 160.
[562] Gün, "Bilişim Suçları", 215.
[563] Soyaslan, *Özel Hükümler*, 632.
[564] Soyaslan, *Özel Hükümler*, 642.
[565] Yılmaz, "5237 Sayılı", 68.
[566] Yılmaz, "5237 Sayılı", 69.

Suç toplumsal düzenin devamı için korunması gereken hukuki değerlerin bilinçli ihlali veya bu değerleri korumaya yönelik kurallara özensizlik oluşturan haksız insan davranışlarıdır[567]. Devletin toplumdaki ortak yaşam şartlarını korumaktan kaynaklanan menfaati ise suçla korunan hukuki değer olarak ifade edilir[568]. Bir suç tipiyle tek bir hukuki değer korunabileceği gibi birden fazla hukuki değeri de koruması amaçlanmış olabilir[569]. Kanaatimce TCK m. 244'te yer alan suçlar ile birden fazla hukuki değer korunmaktadır. Bu kapsamda öncelikle sistemin usulünce çalışmasındaki yarar gözetilerek bilişim sisteminin işleyişi ve kullanıcının veriler üzerindeki tasarruf yetkisi korunmaktadır. Bununla beraber özellikle günümüz koşullarında bilişim sistemlerinin kullanım alanının genişliği ve yaygınlığı da göz önünde bulundurulduğunda toplum güveni, kamu düzeni ve ekonomik düzen, bu suçla korunan önemli hukuki değerlerdir. Kamu düzeni kavramı farklı toplumsal- siyasal koşullara, zaman ve mekana göre değişebilen bir kavram olsa da temelde toplumun maddi bir karışıklık içerisinde olmamasını, huzur ve güvenlik içinde düzen ve uyum halinde bulunmasını sağlayan iç barışı ifade etmektedir[570]. Kamu düzeninin korunması kapsamında temel değerler, genel adap ve ahlak, temel adalet anlayışı, insan hak ve özgürlüklerinin korunması ve bunlara aykırılığın önlenmesi söz konusudur[571]. Hak ve hürriyetleri korumanın devletin temel

---

[567] İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler*, (Ankara: Seçkin Yayıncılık, 2024), 176.

[568] Şenel Sarsıkoğlu, "Halkı Yanıltıcı Bilgiyi Alenen Yayma (Dezenformasyon) Suçu (TCK m. 217/A)", *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, 7/3 (2024): 723.

[569] Şenel Sarsıkoğlu, "Halkı Yanıltıcı", 723.

[570] Fazıl Hüsnü Erdem, "TCK'nun 312. Maddesinin Koruduğu Hukuksal Değerin Kısa Bir Analizi: Türk Devlet Düzeni V. Demokratik Kamu Düzeni", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 52/1 (2003): 38.; Yargıtay benzer bir biçimde kamu düzenini şu şekilde ifade etmektedir: "…*Kamu güvenliği, kamu düzeninin alt kategorisidir. Kamu düzeni, içeriği itibari ile değişken ve nispi olmasına karşın, yine de değişmeyen bir öz'ü içinde taşır. Bu da toplum hayatında maddi bir karışıklığın olmaması, belli bir düzenliliğin, barışın bulunması ve bu haliyle de kamu huzuru-kamu güvenliği ve kamu sağlığını içermesidir. Toplumda düzensizlik ve karışıklığın bulunmaması ve yaşamın normal, doğal akışı içinde geçtiğini belirtmek için, "kamu düzeni", kavramı kullanılır. Kamu düzenini bozan eylemlerin ülke yönünden bütünsellik ve devamlılık göstermesi durumunda kamu güvenliği ile karşı karşıya geliriz. Kamu düzeni "toplum hayatının huzur ve güvenlik içinde yürümesini sağlayan düzenin bir bütünüdür. Başka bir deyişle "kamu düzenine karşı işlenen cürümler kamu huzur ve güvenliğini tehlikeye koyabilen suçlardandır…*"" Yargıtay Ceza Genel Kurulu, 29.04.2008, 2007/8-244 E., 2008/92 K. https://kazanci.com.tr/, E.T. 03.03.2025.

[571] Yargıtay bir kararında kamu düzeninin çerçevesini şu şekilde ifade etmektedir: "…*iç hukuktaki kamu düzeninin çerçevesi, Türk hukukunun temel değerlerine, Türk genel adap ve ahlâk anlayışına, Türk kanunlarının dayandığı temel adalet anlayışına, Türk kanunlarının dayandığı genel siyasete, Türkiye Cumhuriyeti Anayasası'nda yer alan temel hak ve özgürlüklere, milletlerarası alanda geçerli ortak prensip ve özel hukuka ait iyiniyet prensibine dayanan kurallara, medeni toplulukların müştereken benimsedikleri ahlâk ilkeleri ve adalet anlayışının ifadesi olan hukuk prensiplerine, toplumun medeniyet seviyesine, siyasi ve ekonomik rejimine, insan hak ve özgürlüklerine aykırılık şeklinde çizilebilir…*" Yargıtay Hukuk Genel Kurulu, 03.05.2023, 2022/11-277 E., 2023/408 K., https://kazanci.com.tr/, E.T. 03.03.2025.

görevlerinden olduğu anlayışını güden[572] Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin kamu düzeni anlayışının odağında demokratik toplum kavramı yer almakta olup bu kavramın dayanağını İnsan Hakları Evrensel Bildirgesi m. 29 oluşturmaktadır[573]. Bu kavramın unsurlarından birisi olan çoğulculuk unsurunun içerisinde değerlendirilen hürriyetlerden biri de kollektif hürriyetlerdir[574]. Bu kapsamda yalnızca bireysel açıdan hürriyetler değil, devlete ve toplumun bir bölümüne aykırı gelen, zarar verici eylemlere karşı toplumun korunması da bu çerçevede değerlendirilmektedir[575]. Yine bu kapsamda ekonomik düzenin sağlanması da kamu düzeninin içerisinde değerlendirilmektedir[576]. Topluma karşı suçlar bölümünde esasen kamu düzenine karşı suçların düzenlendiği[577] dikkate alındığında kanunkoyucunun bilişim suçlarına kamu düzeninin sağlanması açısından bir değer atfettiği görülmektedir. Yani bilişim suçlarının kanun sistematiğindeki yeri de korunan hukuki değeri yansıtmaktadır.

Mülkiyet hakkı medeni hukuka göre bir eşya üzerinde kurulan mülkiyet ilişkisinden kaynaklanan yetkilerin hukuk düzenince tanınarak korunmasını ifade eden ayni bir haktır[578]. Anayasa m. 35'de kişinin temel hakları içerisinde düzenlenen haklardan birisi de mülkiyet hakkıdır. Bu hak ayrıca AİHS 1 No'lu Protokolü m. 1'de düzenlenmiştir[579]. AİHM ve Anayasa Mahkemesi nelerin malvarlığı ya da "mülk" teşkil edeceği konusunda her türlü ekonomik değeri anayasal mülkiyet hakkı kapsamında görmekte olup[580] mülkiyet kavramını Türk Medeni Kanunu'nda yer alan mülkiyet kavramıyla sınırlı görmemektedir[581]. Bu kapsamda mülkiyet hakkı eşya hukukunda mal olarak kabul edilen şeyler dışında gayrimaddi malvarlığı değerleri ve haklar üzerinde de kurulabilmektedir[582]. Dolayısıyla bilişim suçlarının konusu olan sistemin soyut unsurları üzerinde anayasal anlamda mülkiyet hakkı söz konusudur. Ancak bu unsurlar soyut

[572]Reyhan Sunay, "Avrupa Sözleşmesi Çerçevesinde Oluşan "Avrupa Kamu Düzeni" Kavramının Kapsamı ve Fonksiyonel Değeri", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 7/1-2 (1999): 309.
[573] Sunay, "Avrupa Sözleşmesi", 318.
[574] Sunay, "Avrupa Sözleşmesi", 319.
[575] Sunay, "Avrupa Sözleşmesi", 320.
[576]Altın Aslı Şimşek, "Genel Kamu Hukukunun Temel Kavramı Olarak Kamu Düzeni", (Yüksek Lisans Tezi, Ankara Üniversitesi, 2010), 25.
[577]Zeki Hafızoğulları ve Devrim Güngör, "Türk Ceza Hukukunda Suçların Tasnifi", *Türkiye Barolar Birliği Dergisi*, 69 (2007): 31.
[578] Kürşat Akça, "Anayasa Mahkemesi Kararlarında Mülkiyet Hakkı", *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 6/3 (2016): 552.
[579] Haydar Burak Gemalmaz, *Mülkiyet Hakkı*, (Ankara: Avrupa Konseyi, 2018) ,1.
[580] Gemalmaz, *Mülkiyet Hakkı*, 33.
[581] Gemalmaz, *Mülkiyet Hakkı*, 34.
[582] Akça, "Anayasa Mahkemesi", 580.; Gemalmaz, *Mülkiyet Hakkı*, 34.

olmaları itibariyle medeni hukukta eşya kavramıyla bağdaşmadığı için Türk Ceza Hukuku bağlamında mala zarar verme suçu kapsamında görülemediğinden, bunlar üzerindeki mülkiyet hakkının korunması TCK m. 244 ile sağlanmaktadır.

Görüldüğü üzere TCK m. 244'de yer alan düzenleme birçok farklı hukuki değeri korumaktadır. Bu suçlarla soyut nitelikteki sistem ve veriler üzerindeki mülkiyet hakkının da koruma altına alındığı görülmekle birlikte, korunan hukuki değerin yalnızca mülkiyet hakkı olduğu düşüncesi, bu suçlarla korunmak istenen toplum güveni, sistem bütünlüğü ve ekonomik düzen gibi değerlerin göz ardı edilmesi anlamına gelmektedir. Bu sebeple korunan değerin karma bir nitelik arz ettiği ifade edilmelidir.

TCK m. 244'ün paralel biçimde oluşturulduğu AKSSS m. 4. ve 5'in açıklandığı raporda AKSSS m. 4'de korunan hukuki değerin bilişim sistemlerindeki veri ve yazılımlara zarar verilmesinin önlenerek bunların doğru bir şekilde işlevlerini sürdürmelerini sağlamak olduğu belirtilmiştir[583]. Buna göre; maddi varlığı olan şeylere karşı gerçekleştirilen zarar verici eylemlere karşı getirilen korumaya benzer biçimde, maddi varlığı olmayan bilgisayar veri ve programlarına yönelik korumanın sağlanmak istendiği ifade edilmiştir[584]. Veriye müdahalede ilgilinin veri üzerinde üçüncü kişilerce müdahale edilmesinin önüne geçilerek tasarruf yetkisinin korunduğu, bu korumanın dışa dönük olarak verinin içeriğinin öğrenilmesi ya da verinin üçüncü kişilerce kullanılmasına karşı gerçekleşmesi söz konusuyken, içe dönük olarak veriye müdahale edilerek zarar verilmesine karşı gerçekleşmektedir[585]. AKSSS m. 5'de ise sistem kullanıcılarının sistemi düzgün bir biçimde kullanabilme haklarının korunduğu ifade edilmiştir[586]. Böylece sisteme yönelik eylemler veri ve programlara karşı eylemler açısından ele alınarak; sistemi kullananlarca veyahut sistem operatörlerince sistemin usulünce çalışmasındaki yararlarının korunduğu ifade edilmektedir[587]. Rapora göre, özetle; bilişim sistemlerine karşı gerçekleştirilecek haksız saldırıları önlemek düzenlemenin temel amacıdır[588].

2.3. Suçun Unsurları

[583] Dülger, *İnternet İletişim Hukuku*, 337.
[584] Ketizmen, "Bilişim Suçları", 145.
[585] Ketizmen, "Bilişim Suçları", 146.
[586] Dülger, *İnternet İletişim Hukuku*, 337.
[587] Ketizmen, "Bilişim Suçları", 146.
[588] Apaydın, *Bilişim Ceza Hukuku*, 157.

2.3.1. Suçun Maddi Unsurları

2.3.1.1. Suçun Konusu

TCK m. 244'de ilk iki fıkra arasındaki en önemli ayrımlardan biri suçun konusu olarak karşımıza çıkmaktadır. Buna göre ilk fıkrada suçun konusunu bilişim sistemleri oluştururken; ikinci fıkrada konu sistemde yer alan verilerdir[589]. Bilişim verilerin işlenmesini, diğer bir ifadeyle veri iletişimi ifade eden bir kavram olup; bilgisayarlar, WAP uyumlu cep telefonları, WEB paneli sayesinde ağa bağlanarak bilgi aktarabilen ev aletleri, veri iletişimini sağlayan somut ve soyut ağlar gibi teknolojiler gibi bu amaçla kullanılan teknolojilerin tümüne bilişim sistemi adı verilmektedir[590]. Kanunun böyle geniş bir kavramı kullanarak ileride gerçekleşecek gelişmeleri kapsam altına alması oldukça yerinde görülmekle beraber, 765 sayılı TCK döneminde bilgileri otomatik işleme tabi tutan sistem ifadesinin suçta kullanılamayacak birçok aracı da kapsaması sebebiyle eleştirilmesi dolayısıyla, bilgileri otomatik işleme tabi tutan sistem ifadesine yer verilmeyerek yerine bilişim sistemi ifadesi tercihinin yapılmasının son derece yerinde olduğu belirtilmektedir[591].

Öğretide suçun konusu olan verilerin mutlaka bir bilişim sisteminde yer alan veriler olması gerektiği belirtilerek depolama işlevi gören araçlardaki veriler açısından bu suçun oluşmayacağı, eylemin ancak mala zarar verme kapsamında değerlendirilebileceği öne sürülmüş olup[592]; başka bir görüşte sistemin donanımı içerisinde ana kart, yerel disk gibi birçok donanım unsurunun girdiği, dolayısıyla sisteme takılmak suretiyle kullanılan USB bellek gibi aygıtlardaki verilerin de suçun konusu olarak kabul edilmesi ve mala zarar verme suçuyla TCK 244 arasında fikri içtima yapılarak hareket edilmesi gerektiği savunulmuştur[593]. Kanaatimce de madde lafzında "bir bilişim sistemindeki veriler" ibaresi geçtiğinden, burada bilişim sistemi olarak görülemeyecek, sadece depolama amacına hizmet eden USB bellek gibi aygıtlarda yer alan veriler bu madde kapsamında değerlendirilemeyecektir. Bu durumda

[589] Hasan Tahsin Gökcan ve Mustafa Artuç, *Pratik Türk Ceza Kanunu*, (Ankara: Adalet Yayınevi, 2023), 1322.; Gün, "Bilişim Suçları", 217.
[590] Akbulut, "Sistemi Engelleme", 25.; Yenidünya ve Değirmenci, *Mukayeseli Hukukta,* 31.
[591] Akbulut, "Sistemi Engelleme", 26.
[592] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1045.; Koca ve Üzülmez, *Özel Hükümler*, 1027.; Ketizmen, "Bilişim Suçları", 178.; Muammer Ketizmen, *Türk Ceza,* 143.
[593] Akbulut, *Bilişim Alanında Suçlar*, 189.; Akbulut, "Sistemi Engelleme", 27.

böyle bir eylem mala zarar verme kapsamında değerlendirilebilecek olsa da zarar gören verilerin taşıyabileceği önem dikkate alındığında, sistem haricindeki veriler yönünden bir düzenleme eksikliği bulunduğu ifade edilmelidir.

Doktrinde, TCK m. 244/1 açısından söz konusu eylemlerin yalnızca fiziki varlığı bulunan sistem unsurlarına karşı işlenip işlenmeyeceği konusunda, madde gerekçesinde "aracın fiziki varlığı ve işlemesini sağlayan bütün diğer unsurları" ifadesiyle aksi yönde bir eğilim olduğu düşünülse de; unsur vasfında olmak şartıyla hem yazılım hem de donanımın suçun konusu kapsamında olduğu ifade edilmektedir[594]. Başka bir görüşe göre ise gerekçede zaten diğer unsurlardan açıkça bahsedildiğinden suçun konusunun sadece donanımla kısıtlanmadığı açıktır[595].

Doktrinde bir görüşe göre; bilişim sistemine karşı işlenen eylemlerin düzenlendiği ilk fıkrada suçun konusu olarak bilişim sistemlerinin gösterilmesinin hatalı olduğu, içerisinde hiçbir veri bulunmayan ve çalışabilir durumda bulunmayan bir bilişim sistemine zarar verilmesi halinde, bu suçun konusunu oluşturmayacağından, yanlış bir belirleme yapıldığı savunulmaktadır[596]. Buna göre, maddenin asli düzenlenme amacı klasik mala zarar verme suçu ile koruma altında bulunmayan verilerin korunmasına yönelik olup sistemin donanımına verilen ve mala zarar verme suçu kapsamında değerlendirilebilecek zararları cezalandırmak değildir[597]. Bu sebeple de aracın işlemesini sağlayan bütün diğer unsurların suçun konusunu oluşturacağını ifade eden madde gerekçesinin de bu görüşe göre hatalı olduğu düşünülmektedir[598]. Doktrinde yer alan başka bir görüşe göre ise, içinde veri yer almasa bile bir bilişim sisteminin temel vazifelerini yerine getirebilecek sistemlerin ilk fıkra kapsamında görülmesi gerektiği, aksi halde söz konusu sistemlerin korumadan yoksun bırakılacağı ifade edilmiştir[599]. Farklı bir görüş ise sistemin işleyişini sağlayan donanımsal unsurların bu suç kapsamında değerlendirilemeyeceğini, bu madde ile yalnızca yazılıma yönelik

[594] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1005.; Benzer şekilde; Mahmutoğlu, "Yargı Kararları Işığında", 869.
[595] Karagöz, "Bilişim Sistemini", 114.; Erdoğan, "Engelleme Bozma", 161.
[596] "*...zira bir bilişim sistemi donanım, veri ve ağ unsurlarından oluştuğundan içinde veri bulunmadığından bir bilişim sistemi olarak kabul edilmeyerek bu suçun konusunu da oluşturamayacaktır*."; Dülger, *İnternet İletişim Hukuku*, 339.: Benzer şekilde; Gün, "Bilişim Suçları", 219.; Geçmez, *Değiştirme Suçları,* 91.
[597] Dülger, *İnternet İletişim Hukuku,* 339.
[598] Dülger, *İnternet İletişim Hukuku,* 340.
[599] Karagöz, "Bilişim Sistemini", 114.; Erdoğan, "Engelleme Bozma", 162.

eylemlerin cezalandırılmasının amaçlandığını savunmakta ve donanıma verilen zararların mala zarar verme suçu kapsamında değerlendirilmesi gerektiğini ifade etmektedir[600]. Bu görüşe göre failin kastının yazılıma mı yoksa donanıma mı yönelik olduğu önem arz etmektedir[601]. Başka bir görüşe göre ise gerekçe de dikkate alındığında burada belirtilen eylemler sistemin hem yazılım hem de donanımına zarar verici niteliktedir[602]. Kanaatimce maddenin asli düzenlenme amacı bilişim sisteminin düzgün işleyişi ve sistemdeki verilerin korunması olup salt mala zarar verme amacıyla somut bir bilişim sistemine yönelik gerçekleştirilecek eylemler mala zarar verme suçu kapsamında değerlendirilmelidir. Bununla birlikte fiziksel saldırılarla gerçekleştirilen eylem sonucu soyut nitelikteki unsurlara yönelik bir zarar meydana gelmişse bu durumda TCK m. 244/1-2 açısından failin olası kastının değerlendirilmesi gerekir.

2.3.1.2. Fail

TCK m. 244'de yer alan düzenlemede fail yönünden herhangi bir özel nitelik belirtilmediği görülmektedir. Dolayısıyla herkes bu suçun faili olabilir. Ancak insan dışı varlıkların iradi hareket serbestisi olduğuna yönelik henüz herhangi bir kabul mevcut olmadığından bu suçun faili ancak insan olabilir[603]. Bununla birlikte doktrinde hukuken kişi olarak kabul görmeyen yapay zekanın, suç teşkil eden davranışları sebebiyle üreticinin dahi ceza hukuku bağlamında sübjektif sorumluluk gereği sorumlu tutulamaması, sorumluluğun erimesi olarak adlandırılmakta; bir görüşe göre bu durum objektif isnat edilebilirlik kapsamında izin verilen risk olarak görülmeli, başka bir görüşe göre ise üreticilerin taksirle sorumluluğu olarak değerlendirilmeli, diğer bir görüşe göre ise öngörülebilirlik değerlendirmesi yapılmalıdır[604]. Ancak hukukumuzda bilişim suçlarının taksirle işlenmesi söz konusu olmadığından, bu kapsamda üreticinin cezai sorumluluğuna gitmek mümkün görünmemekle beraber olası kast halinde cezalandırmanın mümkün olabileceği söylenebilir.

---

[600] Apaydın, *Bilişim Ceza Hukuku*, 157.; Benzer şekilde; Hüdaverdi Uçar, "5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları", (Yüksek Lisans Tezi, Çankaya Üniversitesi, 2014), 63.

[601] Apaydın, *Bilişim Ceza Hukuku*, 163.; Gün, "Bilişim Suçları", 219.; Apaydın, *Bilişim Sistemine Girme, Engelleme ve Bozma Suçları*, (Ankara: Seçkin Yayınları, 2023), 167.; Demirci, *Soruşturma Yöntemleri*, 95.

[602] Mehmet Emin Artuk, Ahmet Gökçen ve Ahmet Caner Yenidünya, *Türk Ceza Kanunu Şerhi Özel Hükümler Madde 235-345, 5. Cilt,* (Ankara: Turhan Kitabevi, 2009), 4660.

[603] Karagöz, "Bilişim Sistemini", 116.

[604] Bu konudaki tartışmalar için bkz: Alp Öztekin, *Bilişim Sistemine Girme Suçu*, (Ankara: Seçkin Yayınları, 2023), 151-153.

Doktrindeki bazı görüşlere göre bilişim suçlarının teknik yönü dolayısıyla teknik bilgi gerektiren suçlar olarak "beyaz yaka suçu" olarak değerlendirilmesi gerektiği düşünülmüşse de, günümüzde bu suçların işlenmesinde kullanılan yazılım ve donanımlar az bir çabayla kolayca ulaşılabilir hale geldiğinden, teknik bilgi sahibi olan ya da olmayan kişiler açısından bu suçları işlemede artık pek bir ayırt edici fark kalmamıştır[605]. Bununla birlikte dünya genelinde yapılan bir araştırmaya göre bu suçları işleyen faillerin genellikle 20-30 yaş aralığındaki kimselerden oluştuğu tespit edilmiştir[606].

Failin tespiti için, eylem sisteme yönelikse sistemin, veriye yönelikse verinin, hem sisteme hem veriye yönelikse her ikisinin ayrı ayrı kullanım, mülkiyet ve tasarruf haklarının sahibi ve zararın kimin tarafından meydana getirildiği açık bir şekilde belirlenmelidir[607]. Başkasına ait verilere ve sistemlere zarar verilmesi suçun oluşmasına sebebiyet vereceğinden eylemi gerçekleştirenin kendi veri ve sistemlerine zarar vermesi halinde bu suç oluşmaz[608]. Ancak failin başkasının sisteminde bulunan kendine ait verileri yok etmek için söz konusu sisteme zarar vermesi halinde TCK m. 244/1'deki suç gerçekleşmiş olacaktır. Bu noktada önem arz eden, zarar verilen veri ve sistemlerin üzerinde, fail dışında başka bir kimsenin hak sahipliği veya tasarruf yetkisinin bulunup bulunmadığıdır. Bununla birlikte, doktrinde, failin başkasına ait bir sistemde bulunan kendine ait verilere müdahale etmesi durumunda, veriler sistemden bütünüyle bağımsız düşünülemeyeceğinden faillik sıfatının oluşacağı, failin eyleminin kendiliğinden hak alma olarak değerlendirilmesi ve eylemin hukuka uygunluk nedenleri içerisinde tartışılması gerektiği de ifade edilmiştir[609].

Sistem sahibinin sistemin kullanımını diğer bir şahsa devretmesi örneğinde olduğu gibi zarar gören veri taşıma aracı ve bilişim sistemlerinin malikiyle verinin malikinin aynı kişi olmadığı durumlarda, sistem sahibinin kullanıcının verisine zarar vermek amacıyla kendi mülkiyetindeki sisteme zarar vermesi halinde sistem sahibi; sisteme zarar vermek amacıyla yahut kendi verisini yok etmek amacıyla kullanıcının kasten sisteme zarar

[605] Demircan, *Bilişim Alanında Suçlar,* 43.; Yenidünya ve Değirmenci, *Mukayeseli Hukukta,* 57.
[606] Apaydın, *Bilişim Ceza Hukuku,* 162.; İsmail Tulum, "Bilişim Suçlarıyla Mücadele", (Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, 2006), 46.
[607] Cengiz Apaydın, *Bilişim Sistemine Girme, Engelleme ve Bozma Suçları*, (Ankara: Seçkin Yayınları, 2023), 165.; Akarslan, *Bilişim Suçları*, 49.; Dülger, *İnternet İletişim Hukuku,* 338.
[608] Akbulut, *Bilişim Alanında Suçlar*, 183.
[609] Karagöz, "Bilişim Sistemini", 117.

vermesi halinde ise kullanıcı fail konumunda olacaktır[610]. Burada sistem sahibinin fail olarak eylemde bulunması hali TCK m. 244/2 kapsamında değerlendirilirken[611], kullanıcının fail olarak eylemde bulunması hali TCK m. 244/1 kapsamında değerlendirilir. Veri sahibiyle sistem sahibinin farklı kişi olduğu bu tarz hallerde tasarruf yetkisi bu kişiler arasındaki hukuki ilişki göz önünde tutularak belirlenmelidir[612]. Bu kişiler arasındaki sözleşmeye göre, devredilen verilerde ayni kullanım geçişi de söz konusuysa verilere müdahale suç oluşturmayacaktır[613]; ancak sözleşmede tasarruf yetkisi değil de yalnız verileri sisteme girme yetkisi verilmişse kasti olarak söz konusu verilere zarar verilmesi halinde TCK m. 244/2'deki suça vücut verecektir[614]. Ancak yetki verenin verilerinin bir kopyasını kendisinde tuttuğu görüşüyle; kendisine verilen verilere tasarruf yetkisi olmadığı halde kasten zarar veren veri işleyicinin, bu eyleminin suç oluşturmayacağı yönünde düşünceler de mevcuttur[615]. Yukarıda anlatıldığı tarzda; kullanıcı, sistem sahibi veya veri işleme yetkisi bulunan kişiler arasında gerçekleşen bu tip eylemlerin özellikle bulut bilişim sistemlerinin kullanımının yaygınlaşmasıyla son zamanlarda artış gösterdiği görülmektedir[616].

Özetle; bu suçlarda failin belirlenmesinde önem arz eden husus, TCK m. 244/2 açısından zarar verici eylemi gerçekleştiren kişinin fiili işlediği sırada veriler üzerinde tasarruf yetkisinin bulunup bulunmadığı; TCK m. 244/1 açısından ise sistem ve sistemdeki veriler üzerinde fail dışında mülkiyet, kullanım hakkı ve tasarruf yetkisine sahip olan başka kimseler olup olmadığıdır. Yargıtay'da bu konudaki bir kararında EFT'nin yapıldığı anda IP numarasının hangi kullanıcıya atandığının ve sanıkla irtibatı olup olmadığının tespit edilmesi gerektiğine değinmiştir[617].

Failliğin tespitine ilişkin bir başka durumsa; sisteme yetkisiz şekilde veri yüklenmesi halinde, yetkisiz yüklenen verilere karşı gerçekleştirecek eylemlerin TCK m. 244/2 kapsamında değerlendirilip değerlendirilmeyeceği mevzusudur. Böyle bir durumda; bir

[610] Dülger, *İnternet İletişim Hukuku*, 338.
[611] Akbulut, "Sistemi Engelleme", 20.
[612] Akbulut, *Bilişim Alanında Suçlar*, 184.
[613] Akbulut, "Sistemi Engelleme", 20.
[614] Akbulut, *Bilişim Alanında Suçlar*, 184.
[615] Akbulut, *Bilişim Alanında Suçlar*, 184.
[616] Dülger, *İnternet İletişim Hukuku*, 339.
[617] Karipçin, "Sistemi Engelleme, Bozma", 56; Yargıtay, 11.Ceza Dairesi, 28.01.2009, 2008/16570 E. 2009/101 K, https://kazanci.com.tr/, E.T. 15.01.2025.

kimsenin başka bir kimseye ait bir veri taşıyıcısına yüklemiş olduğu verilerin, veri taşıyıcısı sahibi tarafından silinmesi ya da bu verilere zarar verilmesi halinde veri sahibinin hareketi açısından, bu eylem TCK m. 244/2 kapsamında değerlendirilemeyecek, söz konusu suç oluşmayacaktır[618]. Yine bir başka örnek de; bilişim sistemine teknik destek amacıyla bir kimseye müdahale yetkisi verilmiş olması halinde, bu yetki sınırlı bir yetki olduğundan, teknik destek verecek kişinin kasti olarak verileri yok etme ya da verilere zarar verme eylemlerinde bulunması durumunda da eylem TCK m. 244 kapsamında değerlendirilecektir[619].

2.3.1.3. Mağdur

TCK m. 244'te düzenlenen suç tipinde mağdur yönünden herhangi bir özel nitelik belirtilmediği görülmektedir, dolayısıyla bu suçun mağduru herkes olabilir. Suçun mağduru olmak için mutlak surette zarar gören sistemin yahut verilerin maliki ya da zilyedi olmak gerekmemektedir[620]. Verilere müdahale suçunda verilerin ilgili olduğu kişi tasarruf yetkisine sahip değilse suçun mağduru değil[621], ancak suçtan zarar gören olabilir[622]. Sisteme müdahale açısından mağdur olabilecekler ise kullanıcı, işletici veya sistem sahibidir[623]. Özetle, sistemin ve verilerin, zararsızlık ya da arızasızlık hakkı kime aitse suçun mağduru odur[624].

Doktrinde eylem sonucunda zarar gören bilişim sistemi veya verilerle oluşturulan bilgi, bilimsel çalışma gibi değerlere herhangi bir şekilde ulaşmasında çıkarı olan ve bunlar üzerinde tasarruf yetkisine sahip olan kimsenin bu suçun mağduru olacağı ifade edilmektedir[625]. Aksine düşünceye göreyse; Örneğin, finansal kiralama yoluyla sistemi kullanan kiracının sistem üzerinde mülkiyet hakkı bulunmasa da zilyetlik hakkı bulunması dolayısıyla suçun mağduru olacak, ancak; finansal kiralama şirketi her ne

[618] Akbulut, *Bilişim Alanında Suçlar*, 185.
[619] Demircan, *Bilişim Alanında Suçlar,* 89.
[620] Dülger, *İnternet İletişim Hukuku*, 339.
[621] Akbulut, "Sistemi Engelleme", 21.
[622] Akbulut, *Bilişim Alanında Suçlar,* 185.
[623] Akbulut, *Bilişim Alanında Suçlar,* 185.
[624] Akbulut, "Sistemi Engelleme", 21.
[625] Dülger, *İnternet İletişim Hukuku*, 339.

kadar sistemin maliki olsa da, verileri ve özel alanı ihlal edilen konumunda bulunmadığından suçun mağduru olmayacaktır[626].

Doktrinde bir görüşe göre[627], ancak gerçek kişiler mağdur sıfatına sahip olabileceği için zarar verici eylemin tüzel kişiye ait bir bilişim sistemine karşı işlenmesi halinde, söz konusu tüzel kişi ancak suçtan zarar gören olabileceği ifade edilmektedir. Bu sebeple kamu kurumlarının sahip olduğu bir sisteme karşı bu suçların işlenmesi halinde, ilgili kamu kurumu suçtan zarar gören olacak; sistemin düzgün çalışmasında ve verilerin güvenliğinde menfaati bulunan toplumu oluşturan ilgili herkes ise suçun mağduru konumunda olacaktır[628]. Buna karşın doktrinde eylemlerin bir banka veyahut kredi kuruluşuna ait sistemlere karşı veya bunlar üzerinde gerçekleştirilmesi halinde söz konusu kurum ve kuruluşun suçtan zarar gören değil, mağdur vasfında olacağı düşüncesi de bulunmaktadır[629]. Bu durum da tüzel kişilerin ancak suçtan zarar gören olabileceği düşüncesiyle çelişmekle birlikte, doktrinde tüzel kişilerin de mağdur sıfatına haiz olabileceği düşüncesinde olan bir görüş[630] de mevcut olup, tüzel kişilerin mağdurluk sıfatı öğretide tartışmalı bir konudur[631]. Tüzel kişilerin mağdur olabileceğini[632] savunan görüşe göre suçun doğası elverdiği ve niteliğine uygun düştüğü sürece tüzel kişiler de mağdur olarak değerlendirilebilecektir. Bu konuda TCK m. 244/3 açısından ilgili kurum veya kuruluşun mağdur sıfatına sahip olduğuna yönelik düşünce öğretide baskın olarak yer alan görüştür[633]. Kanaatimce de tüzel kişilerin Türk Medeni

---

[626] Demircan, *Bilişim Alanında Suçlar,* 90.

[627] Akbulut, *Bilişim Alanında Suçlar,* 185.; Gün, "Bilişim Suçları", 217.; Geçmez, *Değiştirme Suçları*, 89.; Koca ve Üzülmez, *Özel Hükümler*, 1026.; Gerçeker, *Ceza Kanunu*, 134.; İzzet Özgenç ve İlhan Üzülmez, *Temel Hukuk Dizisi Ceza Genel Hukuku*, (Ankara: Seçkin Yayıncılık, 2022), 53.; Koca ve Üzülmez, *Genel Hükümler*,1026.; Dülger, *İnternet İletişim Hukuku*, 270.; Alaaddin Egemenoğlu ve Esra Alan, *Ceza Hukuku Temel Kavramlar*, (Ankara: Seçkin Yayıncılık, 2023), 178.; Özgenç, *Genel Hükümler*, 228.

[628] Akbulut, *Bilişim Alanında Suçlar,* 185.; Koca ve Üzülmez, *Özel Hükümler*,1026.

[629] Erdoğan, "Kalma Suçu", 1394.

[630] Erdoğan, "Kalma Suçu", 1394.; Gözde Kaçmaz Keskin, *Türk ve Amerikan Hukukunda Tüzel Kişilerin Ceza Sorumluluğu*, (Ankara: Seçkin Yayıncılık, 2024), 185.; Eylem Baş, *Ceza Hukukunda Fail ve Mağdur,* (Ankara: Seçkin Yayıncılık, 2021), 743.; Gül, *Doğrudan Dolaylı*, 132.; Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1028. Soyaslan, *Özel Hükümler*, 642.; Yaşar, Gökcan ve Artuç, *Yorumlu – Uygulamalı*, 7308.

[631] Karagöz, "Bilişim Sistemini", 115.

[632] Tuğrul Katoğlu, "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları", *AÜHFD*, 61/2 (2012), 672.; Timur Demirbaş, *Ceza Hukuku Genel Hükümler*, (Ankara: Seçkin Yayıncılık, 2023), 608.; Erdoğan, "Kalma Suçu", 1394.

[633] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1044.; Kayaer, "Bilişim Sistemine Girme", 97.; Erdoğan, "Engelleme Bozma", 159.; Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1028.

Kanunu ile kişi olarak kabul edildiği ve hak ve fiil ehliyetleri bulunduğu dikkate alındığında mağdur olmalarının önünde herhangi bir engel bulunmamaktadır[634].

Yargıtay 2. Ceza Dairesi bir kararında, sanığın bir bankanın şubesinde bulunan hesaptan, aynı bankanın bir başka şubesindeki hesabına internet aracılığıyla havale gerçekleştirdiği iddiasıyla açılan kamu davasında, müşteki bankanın her ne kadar yerel mahkemece katılan sıfatı verilmiş olsa da hükmü temyiz hakkı bulunmadığına karar vermiş, gerekçe olarak ise bankanın doğrudan suçtan zarar görmemesini göstermiştir[635].

Medeni hukuka göre mal vasfında görülmediklerinden dolayı veriler üzerinde tasarruf yetkisinin kime ait olduğu doktrinde tartışmalı bir konu olup, bu konuda farklı kıstaslar öne sürülerek yetki sahibi belirlenmeye çalışılmıştır[636]. İlk kıstasa göre verileri hukuka uygun iktisap eden kişinin tasarruf yetkisine sahip olduğu kabul edilmiş, ancak doktrinde yetki sahibi kişinin belirlenmesi açısından yeterli görülmemiş; ikinci kıstasta verilerin içeriğiyle ilgili olan kişinin tasarruf yetkisine sahip olacağı ortaya atılmış, ancak veri girişini yapanla verinin ilgilisinin farklı kimseler olması durumunda yetersiz kaldığı için eleştirilmiş; üçüncü kıstasta veri taşıyıcısının malikinin tasarruf yetkisinin sahibi olacağı ifade edilmiş ancak verilerin başkasına ait olması durumu göz ardı edildiğinden eleştirilmiş; dördüncü kıstasta verinin üreticisinin yani fikri hak sahibinin tasarruf yetkisine sahip olduğu ifade edilmiş, ancak ceza kanununda fikri hakları koruma kanunu bulunmadığından yetersiz görülmüş; son olarak beşinci kıstasta verilerin kaydını ya da naklini gerçekleştiren kişi yetki sahibi olarak belirlenmiş ancak verilerin iktisabında yetersiz görüldüğü için eleştirilmiştir[637]. Görüldüğü üzere tek bir kıstasa bağlı olarak tasarruf yetkisi belirlenememekte, "malik benzeri yetki" olarak ifade edilerek birden fazla kıstas göz önünde bulundurulmaktadır[638]. Bu noktada tasarruf yetkisine sahip olmanın yanında bu yetkinin kapsamı, mutlak bir yetki olup olmadığı da önem arz etmektedir. Kanaatimce tasarruf yetkisine sahip olan kişi ya da kişiler her somut olaya göre değişiklik gösterebileceğinden bu konuda kesin bir kıstas

[634] Benzer şekilde; Katoğlu, "Suçun Mağduru", 673.; Erdoğan, "Engelleme Bozma", 159.
[635]Karagöz, "Bilişim Sistemini", 116.; Yargıtay 2. Ceza Dairesi, 01/06/2016, E. 2014/25924, K. 2016/10421, https://kararara ma.yargitay.gov.tr/, E.T. 15.01.2025.
[636] Akbulut, "Sistemi Engelleme", 22.
[637] Detaylı bilgi için bkz: Akbulut, *Bilişim Alanında Suçlar,* 187.
[638] Akbulut, *Bilişim Alanında Suçlar,* 187.

belirlemek mümkün değildir. Her olayın somut özelliklerine göre ayrı ayrı belirleme yapılması gerekmektedir.

2.3.1.4. Fiil

TCK m. 244'de iki ayrı fıkrada iki ayrı suç tipi düzenlenmiş olup ilk fıkrada bilişim sisteminin işleyişini engelleme ve bozma eylemleri; ikinci fıkrada ise sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi veya başka yere gönderilmesi eylemleri düzenlenmiştir. Burada her iki fıkra için ayrı değerlendirme yapılacaktır.

2.3.1.4.1. Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması (TCK m. 244/1)

TCK m. 244/1'de bir bilişim sisteminin engellenmesi veya bozulması suç olarak düzenlenmiştir. Doktrinde bu suç bir görüşe göre serbest hareketli ve neticeli bir suç iken[639], diğer bir görüşe göre ise bağlı hareketli bir suç olup ancak suç tipinde bulunan hareketin gerçekleştirilmesiyle işlenebilir[640]. Bu suç genellikle icrai hareketle işlenebilecek bir suç olmakla birlikte, teknik sorumlunun koruma için gerekli yazılımları veri işleme engel olmak kastıyla yüklememesi örneğinde olabileceği gibi ihmalen de işlenebilir[641]. Doktrinde bu fıkradaki fiiller yönünden, birlikte hareket etmenin caydırıcılığını sağlamak adına, birden çok bilişim sistemi veya yazılım ile yapılan saldırılarda herhangi bir cezayı artıran düzenlemenin bulunmaması eksiklik olarak değerlendirilmektedir[642].

2.3.1.4.1.1. Engelleme Eylemi

Bir bilişim sistemi amacına uygun faaliyetini yürütürken, dışarıdan yapılan bir etkiyle, bu faaliyetinin kısmen veya tamamen durdurulması "engelleme" olarak ifade edilir[643]. Sistemin işlevine uygun ve doğru bir biçimde yürüttüğü faaliyetine engel olan eylemler bu suçu oluştururken, sisteme yönelik böyle bir etkiye sebebiyet vermeyecek derecedeki

[639] Koca ve Üzülmez, Türk Ceza Hukuku Özel Hükümler, 1027.; Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1045.; Geçmez, *Değiştirme Suçları,* 80.; Dülger, *İnternet İletişim Hukuku,* 342.
[640] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1009.
[641] Hasan Burak Öndin, "Türk Hukukunda Doğrudan Bilişim Suçları", (Yüksel Lisans Tezi, Anadolu Üniversitesi, 2017), 54.; Dülger, *İnternet İletişim Hukuku,* 343.
[642] Demirci, *Soruşturma Yöntemleri,* 99.
[643] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1006.; Koca ve Üzülmez, *Özel Hükümler*, 1028.; Durmuş Tezcan, Mustafa Ruhan Erdem ve Murat Önok, *Ceza Özel Hukuku,* 1045.

eylemler bu suçu oluşturmaz[644]. Engelleme eylemine yönelik olarak doktrinde bir görüşe göre önem arz eden sistemin kısmen yahut tamamen işleyişinin engellenmesi olduğundan, bu eylem, sistemin genel olarak çalışmasını engelleyecek şekilde sistemin herhangi bir parçasının yahut sistemin düzgün çalışmasına katkı sağlayan herhangi bir unsurun düzgün çalışması engellenerek gerçekleştirilebilir[645]. Bu kapsamda verilerin kullanımını, kaydını, depolanmasını, işlenmesini, değerlendirilmesini ya da veri aktarımını önleyici her tür hareket engelleme kapsamında olup; kanunkoyucunun bu konuda bazı hareketlerin cezasız kalmasını önleyebilmek adına geniş bir kavram kullandığı ifade edilmektedir[646].

Doktrinde engelleme eyleminin, zararlı yazılımlarla saldırılar veyahut şifre yerleştirme, mevcut şifreyi değiştirme şeklinde soyut unsurlara yapılacak müdahaleler şeklinde olabileceği gibi sistemin elektriğinin kesilmesi, kablolarının çıkarılması, donanıma ait bir unsurun çıkarılması gibi somut unsurlara müdahale yoluyla da gerçekleştirilebileceği ifade edilmiştir[647]. Buna göre engelleme eylemi sisteme yoğun elektromanyetik dalgalar gönderilmesi ya da müdahale yoluyla işletim sisteminin geçici süre devre dışı bırakılması, iç ağda bilgisayarları birbirine bağlayan kabloların kesilmesi, şifresiz sisteme şifre eklenmesi gibi birçok yöntemle gerçekleştirilebilir[648]. Burada işleyişi engelleme eylemiyle sistemin usulüne uygun çalışmasından kazanılacak her tür faydanın engellenmesi söz konusu olup, sistemi bozmayacak düzeyde ancak sistemin faaliyetini düzgün bir biçimde yerine getirememesine neden olacak şekildeki her tür fiil bu kapsamda değerlendirilir[649]. Buna karşın doktrinde fiziksel müdahalelerin mala zarar verme suçu kapsamında değerlendirilmesi gerektiği, TCK m. 244/1'de yer alan suçun konusunun sistemin soyut unsurları olduğu ve sadece soyut unsurlara yönelik saldırıların bu madde kapsamında değerlendirilmesi gerektiğine yönelik görüşler de mevcuttur[650]. Kanaatime göre; madde metninde bilişim sisteminin engellenmesine yönelik saldırılara ilişkin soyut ya da somut herhangi bir eylem şekli ifade

[644] Yüksektepe, *Soruşturma Usulü,* 460.
[645] Dülger, *İnternet İletişim Hukuku*, 343.
[646] Akbulut, "Sistemi Engelleme", 27.
[647] Dülger, *İnternet İletişim Hukuku*, 343.; İrem Geçmez, *Değiştirme Suçları,* 83.; Erdoğan, "Engelleme Bozma", 176.; Akbulut, *Bilişim Alanında Suçlar,* 191.
[648] Apaydın, Bilişim Sistemine, 171.; Akbulut, *Bilişim Alanında Suçlar*, 191.
[649] Dülger, *İnternet İletişim Hukuku*, 342.; Akbulut, *Bilişim Alanında Suçlar,* 191.
[650] Koca ve Üzülmez, *Özel Hükümler*, 1029.

edilmediğinden, eylemin fiziksel saldırılar yoluyla da gerçekleştirilebilmesi mümkündür.

Doktrinde bir görüşe göre zararlı yazılımlar kullanılarak sistemin yavaşlatılması halinde de sistem engellenmiş olmaktadır[651],Ancak bu görüşe karşın yavaş işleme halini engelleme olarak değerlendirmeyen, sistem işliyor ancak yavaş bir şekilde işliyorsa bu durumda sistemin işlemesinin engellenmediğini ifade eden görüşler de bulunmaktadır[652]. Buna göre; sisteme yapılan müdahale veri işleme faaliyetini kesintiye uğratmış yahut önlemişse sistemin işlemesine engel olunmuş olmakla beraber; sistem işlemeye devam ediyor ancak eskisine göre daha yavaş bir şekilde çalışıyorsa sistemin işlenmesine engel olunmuş olmamaktadır[653]. Yargıtay 11. Ceza Dairesi'nin 2011/2816 E. 2013/4065 K. Sayılı 13.03.2013 tarihinde vermiş olduğu kararında; sistemin verimli çalışmasını engelleyen, faaliyetini ve kapasitesini sınırlandıran, çalışmasını ağırlaştıran ya da kilitleyen eylemler, sistemin işleyişini engellemek olarak değerlendirilmiştir[654]. Kanaatimce de zararlı yazılımlar yoluyla sistemin yavaş işlemesine neden olma halinin, fonksiyon kaybına yol açacağı ve bu yolla kullanıcı açısından zamansal bir engel teşkil edeceği açık olduğundan, bu durumda sistemi engelleme eylemi gerçekleşmiş olacaktır. Bu durumda sistemin işlevselliği kısıtlanarak sistemin normal işleyişi engellenmiş olmaktadır.

Başka bir tartışma konusu ise sistemin geçici ya da kalıcı engellenmesi halinin engelleme eylemi açısından bir fark oluşturup oluşturmayacağı noktasındadır. Bir görüşe göre söz konusu eylemle sistemin işleyişinin geçici olarak mı yoksa kalıcı olarak mı etkilendiğinin belirlenmesi önem arz etmekte olup, sistemin işleyişinin kalıcı olarak sonlandırılması halinde eylemin engelleme değil; bozma kapsamında değerlendirilmesi gerekmektedir[655]. Buna karşın doktrinde diğer bir görüşe göre; sisteme daimi ya da

[651] Mahmutoğlu, "Yargı Kararları Işığında", 866.
[652] Akbulut, "Sistemi Engelleme", 28.; Akbulut, *Bilişim Alanında Suçlar,* 191.
[653] Akbulut, *Bilişim Alanında Suçlar*, 191.
[654]Dülger, *İnternet İletişim Hukuku*, 342.; Akbulut, *Bilişim Alanında Suçlar*, 190.; Yargıtay 11. Ceza Dairesi, 13.03.2013, E. 2011/2816, K. 2013/4065, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.
[655] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1007.; Öndin, "Türk Hukukunda", 54.; Apaydın, *Bilişim Sistemine*, 172.; Geçmez, *Değiştirme Suçları,* 82.; Çakıcı, "M. 243 ve M. 244'te", 327. Erdoğan, *Yargıtay Kararları İle,* 190.

geçici olarak engel olunmasının bir önemi olmadığı ifade edilmekte[656], ancak; geçici engellemenin, yine bu madde kapsamına girmekle beraber, önemsiz ölçüde olması durumunda, haksızlık içeriğinin azlığı sebebiyle cezalandırma dışı bırakılmasına yönelik bir sınırlama getirilmesi gerektiği ifade edilmektedir[657]. Bu düşüncede olanlara göre engelleme eyleminin cezai yaptırımla sonuçlanabilmesi için ciddi ölçüde bir engellemenin söz konusu olması gerekmektedir[658]. AKSSS ise açıklayıcı raporunda bu konuya ilişkin olarak taraf devletlerin engellemenin ciddi ölçüde olması şartı getirilebileceğini belirtilmiş, bununla birlikte asgari düzeyde bir tahribatın dahi ciddi görülebileceği, yavaşlamaya neden olan zararlı yazılım ya da saldırıların ise bu mahiyette ciddi olarak değerlendirilebileceği ifade edilmiştir[659]. Bu konuda farklı bir yaklaşım da engelleme eyleminde hareketin ortadan kalkması halinde sistemin işlevine devam edebilecek olması gerektiği düşüncesindedir[660]. Kanaatimce öncelikle sistemin engellenmesinin kalıcı olmasından ne anlaşılması gerektiğinin irdelenmesi gereklidir. Eylem sonucunda ortaya konulan engelin niteliği, engel ortadan kaldırıldığı takdirde sistemin düzgün işleyişini etkilemiyorsa, bu durumda engelleme söz konusu olacaktır. Böyle bir durumda failin eylemini devam ettirip ettirmemesinin yahut engelin failin eylemini sonlandırması ile ortadan kalkmasının bir önemi yoktur. Ancak engelleme eylemi sonucunda ortaya konan engel, engel daha sonrasında ortadan kaldırılsa dahi, sistemin düzgün işleyişini etkiliyorsa bu durumda sistem bozulmuş olacaktır. Bu kapsamda engelin kalıcı mı yoksa geçici mi olduğu önem arz etmeyip, sistem üzerindeki etkisinin değerlendirilmesi gerekir. Engellemenin önemsiz ölçüde olması durumunda cezalandırılma dışı bırakılmasına ilişkin görüşe ise katılmadığımı ifade etmek isterim. Kanaatimce engelleme 5 saniyeliğine bile gerçekleşmiş olsa, tespit edilebildiği takdirde cezalandırmanın söz konusu olması gereklidir. Burada önemli olan failin eylemi kasten gerçekleştirmiş olmasıdır.

Engelleme eylemine yönelik son olarak; öğretide engellemeye ilişkin düzenlemenin kanunilik ilkesi açısından problemli bir düzenleme arz ettiğini, geniş yorumlama imkanı

---

[656] Demircan, *Bilişim Alanında Suçlar,* 93.; Akbulut, "Sistemi Engelleme", 30.; Gün, "Bilişim Suçları", 222.; Demirci, *Soruşturma Yöntemleri*, 98.; Gökcan ve Artuç, *Ceza Kanunu, 1323.;* Yazıcıoğlu, *Bilgisayar Suçları*, 263. Taşdemir, *Banka veya Kredi*, 269.
[657] Akbulut, *Bilişim Alanında Suçlar*, 193.
[658] Demircan, *Bilişim Alanında Suçlar,* 93.; Eker, "Eski TCK Bağlamında", 125.
[659] Aköz, "Mevzuat Önerileri", 111.
[660] Gün, "Bilişim Suçları", 222.

veren bir kavram olduğunu, engellemenin bir netice olduğunu ve bu neticenin hangi fiillerle gerçekleştirileceğinin AKSSS'de olduğu gibi açıklığa kavuşturulması gerektiğini belirten görüşler vardır[661].

2.3.1.4.1.2. Bozma Eylemi

Bir bilişim sistemine faaliyetini yürütemeyecek bir biçimde kısmen veya tamamen zarar verilmesi durumu "bozma" olarak ifade edilir[662]. Bozma eylemine yönelik olarak Yargıtay 11. Ceza Dairesi; bilişim sistemine dâhil olan mekanik veya yazılımsal unsurunun özgülendiği işlevini gerçekleştiremeyecek hale getirilmesiyle engelleme halinin zirve noktası olan durma noktasından daha ileri bir biçimde çökertme, zarara uğratma, işlemez hale getirme ve hatta fiziki olarak dahi zarar verme olarak ifade etmiştir[663]. Bir sistemin işleyişinin kısmen yahut tamamen sağlıksız hale getirilmesi bozma olarak değerlendirilmektedir[664]. Bir görüşe göre sistemin bozulması; sistemin düzgün faaliyetinin bozulması, çalışması gerekenden farklı çalışması ya da normalden farklı şeyler yapmasının sağlanması, işlevini sistemden beklenildiği gibi gerçekleştiremeyecek, eskisi gibi yapamayacak hale getirilmesi olarak tanımlanmaktadır[665]. Sistemin bozulması ise aynı zamanda zaruri olarak sistemin işleyişinin engellenmesine de neden olmaktadır[666].

Bozma eyleminde dikkat edilmesi gereken husus, verilen fiziki zararın "sistemin işleyişine" verilmesidir[667]. Sistemin unsurlarından bazılarının bozulması sistemin tümünü etkileyecek nitelikte ise, sistemin işlemcisine ya da güç dağıtıcısına etkide bulunmadan temel sistem verilerini barındıran sabit diskin bozulması örneğinde olduğu gibi sistem kendisinden beklenen işlevi göremeyecekse böyle bir durum, bu suç kapsamında değerlendirilir[668]. Eylemin veri düzenini bozma, zararlı yazılım yükleme gibi yöntemlerle mi yahut fiziksel kuvvetle saldırı şeklinde mi gerçekleştirildiği ise

[661] Akbulut, "Sistemi Engelleme", 29.; Akbulut, Bilişim Alanında Suçlar, 192.
[662] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1006.; Koca ve Üzülmez, *Özel Hükümler*, 1028.; Durmuş Tezcan, Mustafa Ruhan Erdem ve Murat Önok, *Ceza Özel Hukuku*, 1045.
[663] Yargıtay 11. Ceza Dairesi, 13.03.2013, E. 2011/2816, K. 2013/4065.
[664] Apaydın, *Bilişim Ceza Hukuku*, 184.
[665] Akbulut, *Bilişim Alanında Suçlar*, 194.
[666] Apaydın, *Bilişim Ceza Hukuku*, 185.; Koca ve Üzülmez, *Özel Hükümler*, 1028.
[667] Demircan, *Bilişim Alanında Suçlar,* 94.
[668] Dülger, *İnternet İletişim Hukuku*, 344.; Benzer şekilde; Akbulut, *Bilişim Alanında Suçlar*, 191.

suçun oluşması açısından önem arz etmez[669]. Sistemin farklı işlemesi ya da yanlış işlemesinin sağlanması da sistemi bozma olarak görülmekte, işleyişinin tamamen yahut kısmen bozulmuş olması ise önem arz etmemektedir[670]. Bununla birlikte doktrinde bir görüşe göre fare, klavye gibi donanım unsurları dışında da, örneğin laptop gibi bir bilişim sisteminin kendisi kırılırsa, her ne kadar sistemin işleyişinin engellenmesi ve bozulması da gerçekleşecek olsa da böyle bir durumda mala zarar verme hükümlerine başvurulması gerektiği savunulmaktadır[671]. Yani bu görüşte bilişim sistemine yapılacak fiziksel saldırıların mala zarar verme suçu kapsamında değerlendirilmesi gerektiği ve TCK m. 244'te yer alan suçun oluşmayacağı düşüncesi mevcuttur[672].

Sonuç olarak TCK m. 244/1'de yer alan suç seçimlik hareketli olarak düzenlenmiş olup sistemin işleyişini bozma veya engelleme eylemlerinin herhangi birinin gerçekleştirilmesi bu suçun oluşması açısından yeterlidir.

2.3.1.4.2. Bir Bilişim Sistemindeki Verilerin Bozulması, Yok Edilmesi, Değiştirilmesi, Erişilmez Kılınması, Sisteme Veri Yerleştirilmesi, Var Olan Verilerin Başka Yere Gönderilmesi (TCK m. 244/2)

TCK m. 244/2'de birden fazla hareket düzenlenmiş olup, bunlar seçimlik hareketlerdir. Sayılan hareketlerden herhangi birinin gerçekleştirilmesi suçun gerçekleşmesi açısından yeterlidir. Bu fıkranın birebir karşılamamakla beraber 765 sayılı TCK'daki m. 525/b-1'in kısmen ise m. 525/a-2'nin karşılığı olduğu ifade edilmektedir[673]. Burada düzenlenin verileri bozma, yok etme, erişilmez kılma ve değiştirme eylemleri söz konusu verilerin kullanımına engel olma amacı taşırken sayılan diğer eylemler bu amacı gütmemektedir[674]. Doktrinde 1. fıkrada yer alan sistemin bozulması eyleminin 2. fıkradaki verilerin bozulması eylemiyle de gerçekleştirilebileceği ifade edilmiş olup; burada fıkralar arasındaki ayrımın temelinin eylemin farklı maksatlarla gerçekleştirilmesi olduğu ifade edilmektedir[675]. Ancak bu kapsamda doktrinde bir görüş, eğer verilere müdahale nedeniyle TCK m. 244/1'deki suç ihlal edilmiş olursa

[669] Dülger, *İnternet İletişim Hukuku*, 344.; Demirci, *Soruşturma Yöntemleri*, 98.
[670] Akbulut, *Bilişim Alanında Suçlar*, 195.
[671] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1046.; Koca ve Üzülmez, *Özel Hükümler*, 1029.
[672] Koca ve Üzülmez, *Özel Hükümler*, 1029.
[673] Öndin, "Türk Hukukunda", 58.
[674] Akbulut, *Bilişim Alanında Suçlar,* 195.
[675] Dülger, *İnternet İletişim Hukuku*, 345.

artık TCK m. 244/2'deki suçun değil, TCK m. 244/1'deki suçun oluşacağını ifade etmektedir[676]. Buna göre ikinci fıkranın uygulanabilirliği için müdahale edilen verilerin sistemin çalışması için olmazsa olmaz bir unsur niteliğinde olmaması ve sistemin fonksiyon kaybına sebebiyet vermemesi gerekmektedir[677]. İkinci bir görüşe göre ise böyle bir durumda burada fikri içtima yapılması gerekmektedir[678]. Başka bir görüşe göre ise 1. fıkradaki eylem 2. fıkradaki eylemle de gerçekleştirilebileceğinden 2. fıkradaki düzenlemenin ilk fıkra olarak düzenlenmesinin, yani fıkraların sıralamasının değiştirilmesinin daha yerinde olacağı ifade edilmektedir[679]. Kanaatimce bu konuda ilk görüş isabetli olup failin saikine göre değerlendirme yapılmalıdır. Failin kastı 2. fıkraya yönelik ise; sisteme yönelik gerçekleşen engelleme, bozma yönünden failin olası kastı değerlendirilmelidir.

TCK m. 244/2'de gerçekleştirilen eylemlerin hareketlerin gerçekleştirme şeklinin önemli olmadığı ve genellikle icrai hareketle işlense de ihmali hareketle de işlenebileceği ifade edilmektedir[680]. Buna göre örneğin; sözleşmeyle sistemi koruma amacıyla icrai davranışta bulunma yükümü altında bulunan bir garantörün saldırıyı fark etmesine rağmen defetmemesi ya da defedecek tedbirleri almaması bu suçun ihmali olarak gerçekleştirmesine sebebiyet verecektir.

2.3.1.4.2.1. Verileri Bozma

Verileri bozma**,** verilerin özgülendiği amaca uygun kullanılmasının tamamen ya da kısmen önüne geçecek şekilde verilere zarar verilmesi eylemini ifade etmektedir[681]. Bu eylem zararlı yazılımlar yoluyla gerçekleştirilebileceği gibi, veri taşıma aracının kırılması suretiyle fiziksel eylemlerle de gerçekleştirilebilir[682]. Birbirine bağlı veri cümlelerinde yer değişikliği yapılarak anlam karıştırma, ilave cümle katma ya da veri cümlelerinde eksiltme yapma gibi şekillerde gerçekleştirilebilir[683]. Veriler kodlardan

[676] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1046-1048.; Koca ve Üzülmez, *Özel Hükümler*, 1030. Erdoğan, "Engelleme Bozma", 172.
[677] Erdoğan, "Engelleme Bozma", 190.; Aköz, "Mevzuat Önerileri", 107.
[678] Değirmenci, "2004 Türk", 205.
[679] Akbulut, *Bilişim Alanında Suçlar,* 195.
[680] Akbulut, *Bilişim Alanında Suçlar,* 201.; Erdoğan, "Engelleme Bozma", 194.
[681] Akbulut, *Bilişim Alanında Suçlar,* 196.; Koca ve Üzülmez, *Özel Hükümler*, 1030.; Ketizmen, " Bilişim Suçları", 171.; Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1009.; Muammer Ketizmen, *Türk Ceza*, 139.
[682] Dülger, *İnternet İletişim Hukuku*, 345.
[683] Akbulut, "Sistemi Engelleme", 32.

oluştuğundan, bu kodlarda yapılan eksiltme ya da değiştirme verinin bozulmasına ve kullanılamamasına yol açacağından, kanun koyucu verinin kısmen veya tamamen tahrip edilmesi açısından bir fark gözetmemiş, bu şekilde her ikisinin de aynı sonuca yol açtığını vurgulamıştır[684].

2.3.1.4.2.2. Verileri Yok Etme

Verileri yok etme**,** verilerin ortadan kaldırılması, silinmesi anlamına gelmekle birlikte[685]; Bir görüşe göre bilişim alanında kullanıldığında "silme" bilinen anlamından biraz daha farklı olarak fiziksel değil, mantıksal anlamda silmeyi ifade etmektedir[686]. Bilişim sisteminde yok etme şekilleri iki tür olup; ilk şekilde veriye ilişkin bütün izler depolama ünitesi üzerinden silinmekte, ikinci şekilde ise veriler depolama ünitesinden silinmemekte, yalnızca veriye erişimi sağlayan anahtar veriler silinmektedir[687]. Buna göre; verilerin silinmesi ile veri tamamen ortadan kaldırılmamakta, üzerine "wipe" denilen işlem ya da yeni veri yazılması işlemi yapılmadıkça sadece dosyalama sistemine göre ulaşım anahtarı değişmekte olduğundan; verilerin silinmesi aslen veriye ulaşımın engellenmesi anlamına gelmekte ve verilerin yok edilmesiyle bu mantıksal silme ifade edilmektedir[688]. Bir görüşe göre kanun koyucunun verileri yok etme ifadesi ile kastettiği her iki tip yok etme şeklinden birinin gerçekleştirilmesidir[689]. Başka bir görüşe göre yok etme sistemde saklanan verilerin tamamen ve telafisi olmayacak şekilde tanınmaz hale getirilmesi, yinelenemeyecek şekilde verilerin ortadan kaldırılması olup, bu ortadan kaldırma hali; verileri oluşturan işaretleme veya bilgilerin ortadan kaldırılması yahut verilerin üzerine yeni veriler yazılması suretiyle asli verinin ortadan kaldırılması yoluyla olabilir[690]. Buna göre kopyası olan verinin silinmesi halinde verinin yok edilmesi gerçekleşmiş olmamakla birlikte[691] güvenlik kopyası bulunan verinin silinmesi halinde suçun oluşacağı ifade edilmektedir[692]. Verinin geri dönüşüm kutusuna atılması halinde bir görüşe göre; veri sistemde bulunmaya devam ettiğinden, sırf yerinin değiştirilmesi

[684] Demircan, *Bilişim Alanında Suçlar,* 97.; Dülger, *İnternet İletişim Hukuku*, 346.
[685] Koca ve Üzülmez, *Özel Hükümler*, 1030.
[686] Erdoğan, "Engelleme Bozma", 197.; Demircan, *Bilişim Alanında Suçlar,* 97.
[687] Yılmaz, "5237 Sayılı", 73.
[688] Dülger, *İnternet İletişim Hukuku,* 346.
[689] Yılmaz, "5237 Sayılı", 73.; Taşdemir, *Banka veya Kredi*, 271.
[690] Akbulut, *Bilişim Alanında Suçlar,* 196.
[691] Akbulut, "Sistemi Engelleme", 33.
[692] Akbulut, *Bilişim Alanında Suçlar,* 197.

niteliğindeki bu hareket ile veri yok edilmiş olmayacaktır[693]. Diğer bir görüş ise böyle bir durumda veri sahibinin veriyi koyduğu yerde bulamaması yeterli olup bu eylem bağlamında yok etme gerçekleşmiştir[694]. Bu konuda kanaatimce her iki tip silme türü ile de yok etme gerçekleşmiş olmakla birlikte verinin kopyasının bulunup bulunmamasının ya da silinen verinin kopya olmasının bir önemi yoktur. Verinin geri dönüşüm kutusuna atılması halinde ise veri dönüşüm kutusunda kaldığı müddetçe veri yok edilmiş olmayacak, bu durumda var olan veriyi başka yere gönderme eylemi gerçekleşmiş olacaktır.

Verilerin yok edilmesi halinde özel bir takım cihazlar veya yöntemlerle verilerin geri getirilebilecek olması durumunda bu eylemin gerçekleşip gerçekleşmediği doktrinde tartışmalıdır. Görüşlerden biri bu şekilde verilerin geri getirilme imkânı söz konusuysa yok etme eyleminin gerçekleşmeyeceğini savunurken[695], başka bir görüşe göre; verinin yok edilmesiyle veriye ulaşmayı normale göre güçleştirecek nitelikteki eylemler kastedilmekte olup, teknik imkânlarla ulaşılabilme imkânı olması suçun oluşmasını engellememektedir[696]. Diğer bir görüşe göre ise verinin kesin bir şekilde yok edilmesi gerekmemekte, erişim için verilen komutun sonuçsuz kalmasına sebep olacak halde kayıtlardan silinmesi yeterli olmaktadır[697]. Madde metninde ise verinin kurtarılabilir olup olmadığına ilişkin bir netice belirlemesi yapılmadığı açıktır[698]. Kanaatimce verinin bu şekilde geri getirilmesi mümkün olsa dahi yok etme eylemi gerçekleşmiş olacaktır. Önemli olan kullanıcının normal yollarla ulaşamayacak hale getirilmiş olmasıdır.

Doktrinde bir görüşe göre verilerin USB bellek gibi bir taşıma aracında bulunduğu hallerde, söz konusu taşıma aracına zarar verilmesiyle veriler yok olursa suç oluşmuş olacaktır[699]. Başka bir görüş ise yalnızca bilişim sistemi sayılabilecek cihazlardaki veriler açısından bu suçun oluşacağını kabul etmekte, depolama aygıtlarındaki verilerin

---

[693] Alaattin Bük, *Bilişim Alanında Kişisel Verilerin Korunması*, (Ankara: Seçkin Yayınları, 2018), 122.; Mahmut Koca, "Hukukumuzda TCK'nun 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", İçinde *Bilişim Hukuku Konferansı* (Ankara: Yargıtay Başkanlığı Yayınları, 2009), 94.; Demirci, *Soruşturma Yöntemleri*, 100.; Koca ve Üzülmez, *Özel Hükümler*, 1030.; Taşdemir, *Banka veya Kredi*, 271.

[694] Erdoğan, "Engelleme Bozma", 198.

[695] Geçmez, *Değiştirme Suçları,* 117.; Akbulut, *Bilişim Alanında Suçlar,* 197.

[696] Koca ve Üzülmez, *Özel Hükümler*, 1030.; Taşdemir, *Banka veya Kredi*, 271.

[697] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1010.; Benzer görüşte; Ketizmen, "Bilişim Suçları", 170.

[698] Aköz, "Mevzuat Önerileri", 113.; Ketizmen, *Türk Ceza*, 139.

[699] Öndin, "Türk Hukukunda", 60.; Kurt, *Açıklamalı - İçtihatlı,* 168. Ali Parlar, *Türk Ceza,* 38.; Soyaslan, *Özel Hükümler*, 644.

ancak söz konusu aygıtın bir bilişim sistemine bağlı olduğu hallerde failce zarar verilmesi halinde bu suçun konusunu oluşturacağını savunmaktadır[700]. Kanaatimce ikinci görüş isabetlidir.

2.3.1.4.2.3. Verileri Değiştirme

Verileri değiştirme**,** veriyi başka bir biçime sokma, başka görünüme ya da duruma getirme, yeni içerik kazandırma anlamına gelmektedir[701]. Değiştirme ile bir veri veyahut veri grubu yerine başkalarının yerleştirilmesi ifade edilmekte olup bilgi notu, resim değiştirme ya da program yazılımını değiştirme şeklinde gerçekleştirilebilir[702]. Verinin içeriğinin değiştirilmeden yalnızca farklı bir program diline çevrilmesi ya da şifre değiştirilmesi yahut silme ile yeni bir durum meydana getirilmesi hali de bu kapsamda görülmüştür[703]. Yine doktrinde bir görüşe göre değişikliğin orijinal veri üzerinde yapılması gerektiği, kopya üzerinde yapılan değişikliklerin bu kapsamda olmadığı da ifade edilmektedir[704]. Veri değiştirmede amaç veriyi yok etmek veyahut erişilmez kılmak değildir, veri değiştirildiğinde sistemin işleyişi devam etmektedir, failin amacı veriye ulaşıldığında yanlış bilgilere erişilmesinin sağlanmasıdır[705].

2.3.1.4.2.4. Verileri Erişilmez Kılma

Verileri erişilmez kılma, bir bilişim sisteminde yahut veri taşıma aracında bulunan verilerin ilgilisi olduğu kişinin bu verilere istediği an ve yerde ulaşmasının engellenmesidir[706]. Burada verilerle ilgili olan kişinin somut kullanım iradesinin tespiti gerekli olmayıp, kişinin potansiyel erişim imkânının ortadan kaldırılmış olması yeterlidir[707]. Doktrinde verilerin erişilmez kılınması tabiri ile ne anlaşılması gerektiği konusunda farklı görüşler bulunmaktadır. Buna göre ilk görüş veriye ulaşması gereken yetki sahibi kimsenin istediği zaman ulaşabilme potansiyelinin engellenmesi olarak değerlendirerek elektriğin kesilmesi, sistemin bozulması, veri taşıma aracının

[700] Erdoğan, "Engelleme Bozma", 186.
[701] Koca ve Üzülmez, *Özel Hükümler*, 1030.
[702] Dülger, *İnternet İletişim Hukuku*, 347.
[703] Akbulut, *Bilişim Alanında Suçlar,* 198.; Benzer şekilde; Koca ve Üzülmez, *Özel Hükümler*, 1030. Ketizmen, "Bilişim Suçları", 172.; Ketizmen, *Türk Ceza*, 140.
[704] Akbulut, *Bilişim Alanında Suçlar,* 198.
[705] Yılmaz, "5237 Sayılı", 74.
[706] Dülger, *İnternet İletişim Hukuku*, 347.
[707] Akbulut, *Bilişim Alanında Suçlar,* 199.

bozulması, verilerin silinmesi gibi birçok eylemi bu kapsamda değerlendirirken[708]; ikinci görüş veriye ulaşmakta kullanılan anahtar sözcüğün değiştirilmesi yoluyla -örneğin şifre değişikliği gibi- yetki sahibinin veriyi kullanamaması olarak değerlendirmekte[709]; üçüncü görüş eylemin şifresiz bir sisteme şifre yerleştirmekle de gerçekleştirilebileceğini ifade etmektedir[710]. Sonuç olarak veri bütünlüğünü korumak amacıyla düzenlenen bu eylem virüs bulaştırma, şifre koyma, verileri silme, başka yere taşıma[711], sistem gücünü kesme yeni giriş engeli konması ya da belirli şekilde kaydedilmiş verilerin adreslerinin silinmesi[712] gibi birçok şekilde gerçekleştirilebilir. Doktrinde 765 sayılı TCK döneminde verilerin fiziki ve mantıki silme olarak ikiye ayrıldığı ve mantıki anlamda silmenin gizlemek kavramı içerisinde verilerin erişilmez hale getirilmesini ifade ettiği, ancak; 5237 sayılı TCK'da erişilmez kılınmanın açıkça düzenlenmiş olması sebebiyle bu ayrımın pek bir önemi kalmadığı ifade edilmektedir[713].

Doktrinde bir görüşe göre verileri silme amacıyla sistemi bozma ya da engelleme hallerinde ilk fıkradaki hükmün uygulanması gerekirken; veri taşıma araçlarındaki verileri silme amacıyla veri taşıma aracının bozulması ya da çalışmasına engel olunması halinde ise, ikinci fıkra hükmü uygulanması gerektiği ifade edilmektedir[714]. Bu görüşe göre veri taşıma aracında bulunan veriler de bu suçun konusunu oluşturabilir[715].

Verilerin geçici yahut sürekli olarak erişilmez kılınması arasında kanunda bir belirleme yapılmadığından suçun gerçekleşmesi yönünden bir fark oluşturmamaktadır[716]. Bununla beraber doktrinde bir görüşe göre sürekli bir engel halinin olması gerektiği savunulurken, genel görüş geçici süreyle engelin de yeterli olduğu kanaatinde olmakla beraber, bu görüşte olanlar sürenin önemli bir zamana tekabül etmesini arayanlar ile

[708] Murat Volkan Dülger, *Bilişim Suçları*, (Ankara: Seçkin Yayınları, 2004), 237.
[709] Kurt, *Açıklamalı - İçtihatlı,* 169.
[710] Koca ve Üzülmez, *Özel Hükümler*, 1030.
[711] Dülger, *İnternet İletişim Hukuku*, 347.
[712] Akbulut, *Bilişim Alanında Suçlar,* 200.
[713] Akbulut, *Bilişim Alanında Suçlar,* 200.
[714] Dülger, *İnternet İletişim Hukuku*, 347.
[715] Dülger, *İnternet İletişim Hukuku*, 347.
[716] Dülger, *İnternet İletişim Hukuku*, 348.

sürenin en azından kesin bir süre ifade etmesinin gerektiğini düşünenler olarak ikiye ayrılmaktadır[717].

2.3.1.4.2.5. Sisteme Veri Yerleştirme

Sisteme veri yerleştirme, sistemde mevcut olmayan dış verilerin sisteme girilmesidir[718]. Sisteme ya da veri aracına dışarıdan ve izin almaksızın hukuka aykırı bir biçimde çeşitli veriler yüklenmesi ya da eklenilmesini ifade etmektedir[719]. Failin sisteme hukuka uygun girmiş olmasının ise bu eylem açısından bir önemi bulunmamaktadır[720]. Örneğin, bir personelin iş yeri sistemine girerek bordrosunda değişiklik yapması bu suçu oluşturur[721].

2.3.1.4.2.6. Var olan Verileri Başka Yere Gönderme

Var olan verileri başka yere gönderme, bir bilişim sisteminde bulunan verileri başka bir sisteme ya da veri taşıma aracına taşımak, kopyalamak eylemlerinde bulunmaktır[722]. Telekomünikasyon yolları[723], wi-fi, bluetooth, USB gibi araçlar aracılığıyla bir sistemde bulunan verilerin başka bir sisteme gönderilmesi yahut veri taşıma cihazına taşınmasıdır. Mağdura ait verinin yine mağdurun bilişim sistemi içerisinde farklı bir dosyaya taşınması halinde de bu suçun oluşacağını ifade eden görüşler mevcuttur[724]. Verilerin nereye taşındığının veyahut failin işine yarayıp yaramadığının bir önemi bulunmamaktadır[725]. Örneğin; sistemden casusluk amacıyla gizli askeri bilgilerin alınması ya da failin işine yaramasa dahi mağdurun özel fotoğraflarını içeren verilerin sistemden alınması halinde bu suç oluşacaktır[726]. Yine, failin sırf denemek amacıyla bir kimsenin bilişim sistemine girerek, hiç işine yaramayacak herhangi bir dosyayı yahut veriyi sistemine transfer etmesi durumunda da bu suç oluşacaktır. Verilerin gönderilmesi sırasında başka hiçbir netice ortaya çıkmasa dahi hareketin kendisi

[717] Bu konudaki tartışmalar için bkz: Akbulut, *Bilişim Alanında Suçlar,* 201.
[718] Akbulut, *Bilişim Alanında Suçlar,* 202.
[719] Dülger, *İnternet İletişim Hukuku*, 350.
[720] Dülger, *İnternet İletişim Hukuku*, 350.; Koca ve Üzülmez, *Özel Hükümler*, 1030.
[721] Öndin, "Türk Hukukunda", 60.
[722] Dülger, *İnternet İletişim Hukuku*, 351.; Koca ve Üzülmez, *Özel Hükümler*, 1030.
[723] Akbulut, *Bilişim Alanında Suçlar,* 202.
[724] Erdoğan, "Engelleme Bozma", 203.; Öndin, "Türk Hukukunda", 61.; Bük, *Verilerin Korunması,* 123.; Taşdemir, *Banka veya Kredi*, 272.
[725] Yılmaz, "5237 Sayılı", 75. Kurt, *Açıklamalı - İçtihatlı,* 170.
[726] Öndin, "Türk Hukukunda", 61. Kurt, *Açıklamalı - İçtihatlı,* 170.

cezalandırılmakta olup, daha ağır bir neticenin ortaya çıkması durumunda oluşan suç nedeniyle cezalandırma söz konusu olacaktır[727]. Serbest hareketle gerçekleştirilebilen bu suçta, eylemin TCK'nın kişisel verilere ilişkin düzenlemelerini içeren TCK m. 135 ve m. 136'dan ayırt edilebilmesi açısından, verilerin niteliğinin belirlenmesi önem arz etmektedir[728].

Doktrinde bir görüşe göre TCK m. 244/2'de düzenlenen sisteme veri yerleştirme ile var olan verilerin başka yere gönderilmesi eylemlerinin fıkrada belirtilen diğer eylemlerle bir ilgisi bulunmadığı ve bu şekilde düzenleme amacının da anlaşılmadığı ifade edilmektedir[729]. Buna göre ya düzenlendiği yerle kavramların bağlantı kurularak ilişkilendirilmesi gerekmekte ya da başka fıkra veyahut bölümde düzenlenmesi gerekmektedir[730]. Başka bir görüşe göre de fıkrada düzenlenen seçimlik hareketlerden en tartışmalısı verinin başka yere gönderilmesi olup hareketin çok muğlak düzenlendiği ve konuluş amacının belirlenemediği ifade edilmekte; bunun sebebi ise, bir sistemde gerçekleşecek her işlemin bir veri iletiminde bulunmasının zorunlu olması dolayısıyla veri iletiminden anlaşılması gerekenin düzenlemeden tam olarak tespit edilememesi olarak görülmektedir[731]. Buna göre; bu hareketin düzenlenmesiyle kanunkoyucunun aslında bu suçları düzenlerken yalnız bilgisayarı düşündüğü anlaşılmakta ve hareketin düzenleniş şeklinin madde ratio legisine hizmet etmekten uzak olduğu ifade edilmektedir[732]. Kanaatimce bu konuda yapılan eleştiriler yerindedir. Maddede düzenlenen bozma, yok etme, değiştirme, erişilmez kılma eylemleri bilişim sistemine karşı gerçekleştirilecek birer sabotaj eylemi niteliğindedir. Bununla birlikte sisteme veri yerleştirme ve var olan verileri başka yere gönderme eylemleri ise birer casusluk eylemi niteliğindedir. Dolayısıyla aynı fıkrada düzenlenmeleri yerinde olmamıştır. Bununla birlikte, kanunkoyucunun kavramları kullanırken belirgin bir tanım yapmaktan kaçınması, eylemlerin tespiti ve sınıflandırılması bakımından belirsizliğe yol açmaktadır.

[727] Demircan, *Bilişim Alanında Suçlar,* 100. Kurt, *Açıklamalı - İçtihatlı,* 170.
[728] Dülger, *İnternet İletişim Hukuku*, 351.
[729] Akbulut, "Sistemi Engelleme", 51.
[730] Akbulut, "Sistemi Engelleme", 52.
[731] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1011.; Aynı görüşte; Erdoğan, "Engelleme Bozma", 205.
[732] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1011.

Verilerin başka yere gönderilmesiyle ilgili olarak belirsizlik oluşturan başka bir konu da verinin aslı ile kopyasının gönderilmesi arasında bir fark olup olmadığıdır. Buna ilişkin olarak doktrinde bir görüş; verinin aslının gönderilmesi halinde, verilerin başka yere gönderilmesi eyleminin değil, verilerin yok edilmesi eyleminin gerçekleşeceğini ifade etmektedir[733]. Buna karşın diğer bir görüş ise gönderilen verinin kopyalanarak ya da kesilerek gönderilmesi arasında fark bulunmadığını ifade etmektedir[734]. Kanaatimce gönderilen verinin asıl veri olması halinde, aynı bilişim sisteminin içerisinde, örneğin başka bir dosyaya gönderiliyorsa, bu durumda eylem verinin başka yere gönderilmesi olarak değerlendirilmelidir. Ancak veri, bulunduğu bilişim sisteminden başka bir bilişim sistemine kesilmek suretiyle gönderiliyorsa bu durumda verinin yok edilmesi söz konusu olacaktır.

Seçimlik hareketlerde sistemden verinin ele geçirilmesine yönelik bir eylemin düzenlemeye konulmamış olması doktrinde bir görüşe göre eksiklik olarak görülmüş[735]; başka bir görüşe göreyse verilerin başka yere gönderilmesi fiilinin zaten verileri ele geçirmeyi de kapsadığı değerlendirilerek bu konuda bir eksiklik bulunmadığı ifade edilmiştir[736]. Bununla birlikte ilk görüşte olanlar verinin kopyalanmak suretiyle başka bir yere gönderilmesi halinde gerçekleşecek olan casusluk eyleminin verilerin başka yere gönderilmesi eylemiyle karşılanacağını, ancak bununla birlikte veriyi herhangi bir yere göndermeden sadece öğrenerek amacına ulaşacak olan failin eyleminin bu korumanın içerisinde olmayacağı ifade edilmektedir[737]. Kanaatimce bu konuda ilk görüş isabetlidir. Fail hukuka aykırı şekilde bilişim sistemine girdikten sonra TCK m. 244/2 kapsamında herhangi bir eylemde bulunmadan yalnızca görerek verinin içeriğini elde edebilir. Bu durumda sisteme girme bakımından cezalandırılması söz konusu olacaksa da verinin içeriğini ele geçirmesi yönünden verilerin kişisel veri niteliğindeki veriler olması hali ile TCK m. 328. maddeler kapsamına giren haller hariç olmak üzere herhangi bir yaptırımla karşılaşmayacaktır. Failin sisteme hukuka uygun girmiş olması

[733] Dülger, *İnternet İletişim Hukuku*, 351.
[734] Gökcan ve Artuç, *Ceza Kanunu*, 1324.
[735] Yazarlar ayrıca eski TCK 525/a maddesinde böyle bir düzenlemenin olduğunu, ancak yeni TCK'da unutularak eksiklik haline geldiğini belirtmektedir.: Avşar ve Öngören, *İnternet Hukuku*, 108.; Değirmenci, "2004 Türk", 208.
[736] Pallı, "Hukukta Bilişim Suçları", 181.
[737] Pallı, "Hukukta Bilişim Suçları", 182.

halinde ise hiçbir yaptırımla karşılaşmayacaktır. Bununla birlikte bu durumun temelinde verilerin hukuk düzenindeki yerinin netleştirilememesi sorunu bulunmaktadır.

TCK m. 244'te yer alan eylemlere ilişkin bir diğer husus da yapılan bir hareketle birden fazla kavramın ihlal edilebilmesi dolayısıyla, eylemlerin ayrımının yapılmasının kolay olmamasıdır. Bir verinin yok edilmesi aynı zamanda aynı veriyi erişilemez hale getirmiş olmakta, hatta bu verinin sisteme ait bir veri olması durumunda sistemin işleyişine engel olmaktadır. Kavramların belirlenmesi noktasında kanun koyucunun geniş bir alan bırakarak söz konusu eylemlerin cezasız kalmasını önlenmesi ve korumada açıklık bırakılmamasını sağlamaya çalıştığı ifade edilmekle birlikte; bu tarz bir düzenlemenin, yapılan hareketle hangi eylem veya eylemlerin ihlal edildiğinin anlaşılması noktasında kafa karışıklığına yol açtığı belirtilmektedir[738]. Doktrinde bir görüşe göre bu durumun çözümünün hem içtima hem de kavramlar göz önünde bulundurularak yapılması gerektiği, öncelikle eylemin fıkrada düzenlenen hangi eylemleri ihlal ettiğinin tespit edilmesi, birden fazla ihlal varsa daha özel olanı belirlenerek tercih yapılması, eylemin her iki fıkra kapsamına da girmesi halinde ise sorunun içtima yapılarak çözümlenmesi gerektiği ifade edilmiştir[739]. Başka bir görüşe göre ise korunan hukuki değer, suçun konusu ve failin saiki ortaya konularak bu karışıklık sorunun çözülmesi gerektiği belirtilmektedir[740]. Ayrıca eylemin ikinci fıkra kapsamında değerlendirilebilmesi için ilk fıkra kapsamına girmiyor olması gerektiği, diğer bir anlatımla; düzenlenen suçların serbest hareketli suç olmaları dolayısıyla neticenin sistemi engelleme veya bozma derecesine ulaşması halinde eylemin ilk fıkra kapsamında değerlendirilmesi gerektiği ifade edilmektedir[741]. Yargıtay TCK m. 244/2'de düzenlenen suça ilişkin olarak; failin eyleminde, maddede yer verilen fiillerden hangileri kapsamında hareket edip etmediği konusunun net bir biçimde belirlenmesi gerektiğini belirtmekte ve bu incelemenin yapılmamış olmasını eksik inceleme olarak değerlendirmektedir[742].

TCK m. 244'de yer alan kavramların ve eylemlerin birbirine yakınlığının çıkardığı görüş ayrılıkları Yargıtay kararlarına da yansımıştır. Yargıtay 23. Ceza Dairesi bir

[738] Dülger, *İnternet İletişim Hukuku*, 352.
[739] Akbulut, *Bilişim Alanında Suçlar,* 202.; Benzer şekilde; Gün, "Bilişim Suçları", 225-228.
[740] Dülger, *İnternet İletişim Hukuku*, 352.
[741] Dülger, *İnternet İletişim Hukuku*, 354. Karagülmez*, Bilişim Suçları,* 239.
[742] Gün, "Bilişim Suçları", 230.; Yargıtay 8. Ceza Dairesi, 11.01.2017 , E: 2016/8498, K: 2017/175, https://kararara ma.yargitay.gov.tr/, E.T. 15.01.2025.

kararında; sanığın katılana ait facebook hesabındaki verilerde herhangi bir değişiklik ya da bozma eyleminde bulunmadan, hesap şifresini değiştirerek hesap sahibi gibi hareket etmesinden ibaret olan eyleminin yerel mahkemece TCK m. 244/2 kapsamında değerlendirilmesini hatalı bularak, TCK m. 244/1 kapsamında sistemin işleyişini engelleme olarak değerlendirmiştir[743]. Yargıtay 15. Ceza Dairesi ise benzer bir olayda "*sanığın, şikâyetçinin elektronik posta adresinin ve facebook hesabının şifresini kırarak, hesaba giriş şifresini değiştirerek erişimini engellemesi şeklinde gerçekleşen eyleminin TCK'nın 244/2. maddesi kapsamında kaldığı halde aynı Kanun'un 244/1. maddesinden mahkûmiyet hükmü kurulması...*" gerekçesiyle bozma kararı vermiştir[744]. Verilen örnek kararlardan anlaşılacağı üzere sosyal medya hesabına erişilerek şifrenin değiştirilmesi ve erişim engellenmesi olarak gerçekleşen benzer olaylarda, Yargıtay'ın iki farklı dairesince birbirine zıt kararlar verildiği görülmektedir. Bu konuda bir değerlendirmede bulunulacak olursa kanaatimce hesap şifresinin değiştirilmesi nedeniyle bir kimsenin hesabına ulaşamayacak hale getirilmesi durumunda burada sistemi engelleme eylemi değil verilere erişimin engellenmesi eylemi söz konusu olacaktır. Çünkü bu halde kişi yalnızca kendi hesabında yer alan verilere ulaşamamaktadır. Ancak kişinin sisteme erişimi halen devam etmekte, yeni bir hesap oluşturabilmekte veyahut başka bir hesapla sisteme erişimi mümkün olabilmektedir. Dolayısıyla failin eylemi TCK 244/2 kapsamında değerlendirilmelidir.

2.3.1.5. Netice

TCK m. 244'de düzenlenen suçların netice unsuru doktrinde tartışmalıdır. Bu konuda ilk görüşe göre; TCK m. 244'te yer alan her iki suç tipinde de eylemler suçun netice unsurunu oluşturmakta olup söz konusu suç neticeli bir suçtur, neticeyi gerçekleştirmeye elverişli her tür hareketle gerçekleştirileceğinden dolayı da serbest hareketli bir suçtur[745]. Kanunda yer alan hareketlerden birkaçının aynı anda

[743] Yargıtay 23. Ceza Dairesi, 24.05.2016, E. 2015/9146, K. 2016/6542, https://kazanci.com.tr/, E.T. 15.01.2025.
[744] Yargıtay 15. Ceza Dairesi, 27.2.2018, E. 2017/35938, K. 2018/1367, https://kazanci.com.tr/, E.T. 15.01.2025.; Bkz. benzer şekilde; Yargıtay 15. Ceza Dairesi, 17.4.2018, E. 2017/9049, K. 2018/2662, https://kazanci.com.tr/, E.T. 15.01.2025.; Yargıtay 15. Ceza Dairesi, 20.3.2018, E. 2017/3157, K. 2018/1848, https://kazanci.com.tr/, E.T. 15.01.2025,; Yargıtay 15. Ceza Dairesi, 19.10.2020, E. 2017/26427, K. 2020/10070, https://kazanci.com.tr/ , E.T. 15.01.2025,; Yargıtay 15. Ceza Dairesi, 17.05.2021, E. 2017/37090, K. 2021/5186, https://kazanci.com.tr/, E.T. 15.01.2025.
[745] Dülger, *İnternet İletişim Hukuku*, 355.; Akbulut, *Bilişim Alanında Suçlar*, 190.; Koca ve Üzülmez, *Özel Hükümler*, 1027.; Erdoğan, "Engelleme Bozma", 192.

gerçekleşmesi durumunda tek suç işlenmiş olacak ve faile tek ceza verilecektir[746]. Bu konuda bir görüşe göre; hareketlerin tek tek sayılmaması ve sınırların tam olarak ifade edilmemesi, sadece netice belirlemesi yapılarak fazla genişlik bırakılması kanunilik ilkesi açısından problem arz etmektedir[747]. Suçun neticeli suç olduğunu savunan görüşlerden birine göre; ilk fıkradaki bozma eyleminde suç tipinde yer alan hareketin sonucunda bozulmanın gerçekleşmesi şart olup mağdurun sistemi kullanamama ihtimalinin ortaya çıkması dahi bir neticeyi ifade etmektedir[748]. Diğer bir görüşe göre; bu hareket sonucunda meydana gelen bozma hali netice olarak değerlendirildiğinde, bozmanın gerçekleşmesi bir zararın oluşmasını ifade ettiğinden, bu suç ayrıca bir zarar suçudur[749]. Başka bir görüş ise; bozma sonucu bir zararın meydana gelmesinin mutlak bir sonuç olmadığı, AKSSS'de sistemin sekteye uğratılmasından bahsedilmiş olup zararın meydana gelmesine yönelik böyle bir belirleme yapılmadığı, suç tipi açısından böyle bir zararın aranmasının suç kapsamını daraltacağı, ayrıca zararın tespitinin belirlenmesi sorununu ortaya çıkaracağı gerekçesiyle bu suçun bir tehlike suçu olduğunu ifade etmektedir[750]. Yine bu görüşe katılan başka bir görüş de; suç tipinde herhangi bir zarar aranmadığını, korunan menfaatin ihlalinin suçun gerçekleşmesi için yeterli olduğunu ifade etmektedir[751]. Yine benzer bir görüşte de; sistemde eylemler sonucunda zarar gerçekleşip gerçekleşmemesinin suçun oluşması açısından önem arz etmeyip ancak cezanın ağırlığı noktasında dikkate alınabilecek bir husus olduğunu ifade etmektedir[752]. Mütemadi suç olarak işlenmesi de mümkündür[753].

İkinci görüşe göre ise; ise suç tipinde ayrıca neticenin gerçekleşmesi gerektiğine dair bir açıklık bulunmadığından, gerçekleşen bir zarar da aranmadığından, bu suç sırf hareket suçu[754] olup; ancak tipte yer alan eylemlerle gerçekleştirilebileceğinden de bağlı hareketli bir suçtur[755]. Başka bir görüş bu suçun neticesi harekete bitişik suç şeklinde

[746] Demircan, *Bilişim Alanında Suçlar,* 101.
[747] Akbulut, *Bilişim Alanında Suçlar*, 192.
[748] Apaydın, *Bilişim Ceza Hukuku*, 187.
[749] Erdoğan, "Engelleme Bozma", 212.; Benzer şekilde; Geçmez, *Değiştirme Suçları,* 86.; Öndin, "Türk Hukukunda", 55.; Gün, "Bilişim Suçları", 220.; Demircan, *Bilişim Alanında Suçlar*, 101.
[750] Pallı, "Hukukta Bilişim Suçları", 170.
[751] Apaydın, *Bilişim Ceza Hukuku*, 189.
[752] Dülger, *İnternet İletişim Hukuku*, 355.
[753] Demircan, Bilişim Alanında Suçlar, 101.
[754] Çakıcı, "M. 243 ve M. 244'te", 329.; Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1009.
[755] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1009.

olduğunu[756] ve bir zarar suçu olmadığını[757] ifade edilmektedir. Yine bu konuda başka bir görüş bu maddede düzenlenen suçların yeni veri yerleştirme eylemi hariç olmak üzere zarar suçu olduğunu ifade etmektedir[758].

Kanaatimce bu konuda birinci görüş isabetlidir. Birinci fıkrada sistemin engellenmesi ve bozulması, ikinci fıkrada verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme eylemleri aslında bir netice ifade ettiğinden, zararlı yazılım kullanarak yahut bunun gibi farklı birçok şekilde gerçekleştirilebileceğinden, bu suçlar serbest hareketli ve neticeli suçlardır. Özellikle bir zararın ortaya çıkması şart değildir. Gerçekleştirilen suç sonucunda ortaya bir zarar çıkabileceği gibi, çıkmaması da mümkün olduğundan söz konusu suçlar tehlike suçudur.

Zarar suçu - tehlike suçu ayrımı neticenin gerçekleştiği yerin tespiti konusunda da önem arz etmekte olup; bu suçların zarar suçu olarak kabul edilmesi halinde somut tehlikenin gerçekleştiği yer neticenin meydana geldiği yer olarak kabul edilecekken, suçun soyut tehlike suçu olarak kabulü halinde -özellikle de uluslararası işlenen suçlarda- suçun işlendiği yerin tespiti sorun olarak ortaya çıkabilecektir[759].

2.3.1.6. Suça Etki Eden Nedenler

2.3.1.6.1. Suçun Bir Banka veya Kredi Kurumuna ya da Bir Kamu Kurum veya Kuruluşuna Ait Bilişim Sistemi Üzerinde İşlenmesi (TCK m. 244/3)

Kişisel bir bilişim sistemine karşı gerçekleştirilecek saldırıların sistem maliki ya da kullanıcısının büyük zararlara uğramasına yol açabileceği şüphesizdir. Ancak failin büyük çaplı kurumsal bir sisteme saldırması halinde ortaya çıkan zararlar çok daha yıkıcı olabilmekte ve geniş kitleleri ilgilendirecek düzeyde zararlara yol açabilmektedir. Bu sebeple, 765 sayılı TCK döneminde, m. 525/b-1'de kişisel bilgisayarlar ile kurumsal bilgisayarlar arasında yapılan bir ayrımın olmaması doktrinde eleştiri konusu olmuş;

[756] Akıncı, Alıç ve Er, "Bilişim Suçları", 241.; Yazıcıoğlu, *Bilgisayar Suçları*, 264.
[757] Yazıcıoğlu, *Bilgisayar Suçları*, 264.
[758] Yaşar, Gökcan ve Artuç, *Yorumlu – Uygulamalı*, 7310, 7314.
[759] Özbek, "İnternet Kullanımında",122.

ortaya çıkacak zararlar arasında büyük farklar olması dolayısıyla kişisel bilgisayarlar ile kurumsal bilgisayarlara eşit muamele yapılmasının hatalı olduğu öne sürülmüştür[760].

5237 sayılı TCK'da ise bu eleştiriler dikkate alınarak; sistemi bozma, engelleme, verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme fiillerinin bir banka, kredi kurumu, kamu kurum veya kuruluşuna ait sistemler üzerinde işlenmesi durumunda faile verilecek cezanın yarı oranında arttırılması öngörülerek TCK m. 244'te yer alan suçun nitelikli hali düzenlenmiştir. Böyle bir ağırlaştırıcı nitelikli halin getirilmesindeki gaye, günümüzde bankalar, kredi kurumları ve idare tarafından yerine getirilen hizmetlerin birçoğunun bilişim sistemleri vasıtasıyla sürdürülmesi ve bu hizmetlere ilişkin kayıtların bilişim sistemlerinde tutulması dolayısıyla, bu sistemlere karşı yapılacak bozma veya engellemeye yönelik eylemlerin diğer sistemlere karşı yapılacak eylemlerden daha ağır neticelere sebebiyet verecek olmasıdır[761]. Örneğin, tapu dairesince kullanılan bir bilişim sisteminin failce engellenmesi halinde engelleme hali ortadan kaldırılana kadar işlem yapılması mümkün olmayacak, bu süreçte bir veya birkaç kişi değil, tapuda işlem yapmak isteyen her vatandaş mağdur olacaktır[762]. Doktrinde yalnızca fıkrada belirtilen kurum ve kuruluşlarla sınırlama yapılmasının doğru olmadığı bir şirket ya da işletmenin sistemlerinin etkilenmesi halinin de büyük zarara yol açabileceği; ayrıca cezanın yarı oranında artırımını öngören sabit artırım sisteminin yerine alt ve üst sınır belirlemesi yapılarak eylemin ağırlığına göre artırım miktarının belirlenmesinin daha yerinde olacağı ifade edilmiştir[763]. Benzer başka bir görüşte ise kritik altyapı olarak belirlenen hizmetlerin yalnızca kamusal tarafta yürütülen hizmetlerle sınırlı olmadığını, kamu özel ayrımı yapılmaksızın bir bütün şeklinde hizmetin korunmasına yönelik düzenleme yapılması gerektiği vurgusu yapılmıştır[764]. Ayrıca; doktrinde bu nitelikli halin yanı sıra, kamu, banka ya da kredi kurumu görevlilerince bu tarz eylemlerin gerçekleştirilmesi halinin, dışarıdan müdahaleye göre çok daha kolay bir şekilde içeriden eylemde veya ihmalde bulunarak kendilerine duyulan güveni kötüye kullanabilecek olmaları

[760] Dülger, *İnternet İletişim Hukuku*, 356.
[761] Erdoğan, "Engelleme Bozma", 167.; Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1012.; Dülger, *İnternet İletişim Hukuku*, 357.
[762] Ömer Demir, Mehmet Arıç ve Halil Polat, *Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar*, (Ankara: Adalet Yayınevi, 2015), 21.
[763] Akbulut, *Bilişim Alanında Suçlar,* 206.
[764] Gün, "Bilişim Suçları", 240.

dolayısıyla, cezayı arttıran bir nitelikli hal olarak düzenlemesi gerektiği ifade edilmektedir[765].

Fıkrada belirtilen kurum ve kuruluşlarla sınırlama yapılmasının doğru olmadığı konusunda yapılan eleştiri son derece yerindedir. Günümüzde özel şirketlere karşı yapılacak herhangi bir siber saldırı oldukça yıkıcı etkilere yol açabilmektedir. Kaldı ki kritik alanlarda faaliyet gösteren şirketlere yapılacak saldırılar yalnızca o şirketi değil, bir ülkeyi hatta dünya genelini etkileyecek zararlara yol açabilmektedir. Özellikle finansal veriler, ticari sırlar gibi kritik verilerin çalınması, tahrip edilmesi, kritik sistemlerin çökertilmesi gibi hallerde üretim süreçlerinin aksaması, ticari itibar kayıplarının oluşması, rekabet ortamının zarar görmesi söz konusu olabilmektedir. Bu durumda piyasalarda büyük dalgalanmalara yol açarak ülke ekonomisi üzerinde zincirleme etkilere sebep olabilmektedir. Yine küresel boyutta tedarik zincirinin aksamasına sebep olarak global ekonomik sorunlara yol açabilmektedir. Özellikle büyük bilişim şirketlerine yapılacak saldırılar, bu şirketlerle verilen hizmetlere bağlantılı olarak iletişim, enerji ve ulaşım gibi kritik hizmetlerin aksamasına yol açabilmektedir. Bu durumun ciddiyetini çok net bir şekilde ortaya koyan bir olay 19 Temmuz 2024'te yaşanmıştır. CrowdStrike olayı olarak adlandırılan bu siber olayda Microsoft'a siber güvenlik hizmeti veren CrowdStrike adlı şirketin yayımladığı bir güncelleme altyapı sorunlarına yol açarak Windows işletim sisteminin çökmesine sebep olmuştur[766]. Dünya genelinde hava yollarını etkilemiş, rezervasyon ve biletleme sistemlerinin çökmesine, uçuş gecikmelerine ve iptallere yol açmıştır. Banka ve finansal kuruluş işlemlerinde gecikmelerin yaşanmasına ve bazı hizmetlerin durmasına neden olmuştur. Sağlık sektöründe hastane bilgi sistemleri ve hasta kayıtlarını erişilemez hale getirmiş, televizyon yayınlarında kesintilere neden olmuş ve daha birçok sektörü etkilemiştir. Bu olay kritik öneme sahip bilişim sistemlerine karşı gerçekleştirilecek herhangi bir saldırının ne kadar yıkıcı etkileri olacağının somut bir örneği olmuştur. Dolayısıyla TCK m. 244/3'te düzenlenen nitelikli hal banka, kredi kurumu, kamu kurum ve kuruluşuna ait sistemler açısından yerinde bir düzenleme oluştursa da, kamu özel ayrımı

[765] Dülger, *İnternet İletişim Hukuku*, 357.; Apaydın, *Bilişim Sistemine*, 174.; Erdoğan, "Engelleme Bozma", 166.

[766] Devrim Danyal, "Crowdstrike ve Microsoft güncellemesi nasıl global sistem krizine dönüştü?", *Anadolu Ajansı*, 15.01.2025, https://www.aa.com.tr/tr/analiz/crowdstrike-ve-microsoft-guncellemesi-nasil-global-sistem-krizine-donustu/3280058.

yapılmaksızın bir bütün şeklinde hizmetin korunmasına yönelik olarak tekrar düzenlenmesi son derece yerinde olacaktır. Cezanın belirlenmesi noktasında ise yalnızca bu nitelikli halle sınırlı olmaksızın, TCK m. 244'ün, genel olarak yetersiz kaldığını ifade etmek gerekir.

TCK m. 244'de yer alan suçların TCK m. 244/3'te yer alan kurumlarda görevli kişilerce bu kurumların sistemlerine karşı gerçekleştirilmesi halinin nitelikli hal olarak düzenlenmesi gerektiği görüşü de son derece yerindedir. Bununla birlikte TCK m. 244/3'te yer alan nitelikli halin tüm hizmetin korunmasına yönelik olarak düzenlenmesi gerektiği düşüncesiyle bağlantılı olarak, kamu görevlileri bakımından getirilecek nitelikli halin kritik hizmet faaliyetini yürüten özel şirketlerde çalışan kişileri de kapsar nitelikte oluşturulması gerekmektedir. Çalışanların çalıştıkları yerdeki sistemlere daha kolay erişim sağlaması, sistemlerin zayıf noktalarını ve açıklarını bilmesi, sisteme erişim yetkilerinin bulunması, veri yapısının ve verinin nerede saklandığının bilinmesi; bu kişilerin suçu işlemesini, diğer kişilere nazaran daha kolay hale getirmektedir. Bununla birlikte bu kişiler, çalıştıkları kuruma karşı gerçekleştirmiş oldukları eylemle, iş akdi ile kurulan güven duygusunu kötüye kullanmış olmaktadır. Ayrıca bir kuruluşun bilişim sistemlerine içeriden müdahalede bulunulması, dışarıdan yapılacak bir saldırıya göre çok daha yıkıcı etkilere neden olabilmektedir. Tüm bu sebeplerle böyle bir nitelikli halin düzenleme altına alınması hem caydırıcılık hem de kusurun ağırlığı dikkate alındığında son derece yerinde olacaktır.

Bu nitelikli halin uygulanabilmesi için eylemlerin bir kamu kurum veya kuruluşuna ya da bir banka veya kredi kurumuna karşı işlenmesi gerekmekte olup[767]; doktrinde banka veya kredi kurumu niteliğinde bulunmayan özel kuruluşlar ile dernek ve vakıfların sistemlerine karşı söz konusu suçun işlenmesi durumunda bu nitelikli halin uygulanmaması gerektiği vurgulanmaktadır[768]. Nitelikli halde geçen banka ifadesine mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankaları; kredi kurumu ifadesine katılım bankaları ile mevduat bankaları; kamu kurum ve kuruluşları ifadesine

[767] Koca ve Üzülmez, *Özel Hükümler*, 1032.
[768] Dülger, *İnternet İletişim Hukuku*, 355.

ise merkezi idare, yerel yönetimler, hizmet yerinden yerel yönetimler de dâhil tüzel kişiliği olup olmadığına bakılmaksızın tüm idari kuruluşlar girmektedir[769].

2.3.1.6.2. TCK m. 244'te Yer Alan Suçun Terör Amacıyla İşlenmesi

TCK m. 244'e ilişkin başka bir nitelikli hal 3713 sayılı Terörle Mücadele Kanunu'nda düzenlenmiştir[770]. Terörle Mücadele Kanunu m. 4'te terör amacıyla işlenen suçlar başlığı altında *"Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak…"* amaçlarıyla bir terör örgütünün faaliyeti çerçevesince TCK m. 244'te yer alan suçun işlenmesi terör suçu olarak nitelendirilmiş; aynı kanunun 5. maddesinde ise böyle bir durumda faile fiili için verilecek hapis cezaları veya adlî para cezalarının yarı oranında arttırılacağı ifade edilmiştir. Bu madde hükümleri çocuklar hakkında uygulanmaz[771].

2.3.1.6.3. Bilişim Sistemi Aracılığıyla Haksız Çıkar Sağlamak

TCK m. 244/4'te; ilk iki fıkrada tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunacağı düzenlenmiştir. Doktrinde bu düzenlemenin ayrı bir suç mu yoksa TCK m. 244'ün ilk iki fıkrasındaki suçların nitelikli hali mi olduğu noktasında görüş ayrılıkları bulunmaktadır.

İlk görüşe göre, TCK m. 244/4'te yer alan düzenleme cezayı artırıcı bir neden olarak düzenlenmiştir[772]. Bu görüşü savunanlara göre kanun oluşturma tekniğinin bir sonucu olarak önce suçun temeli yani basit şekli, daha sonra ise türemiş şekilleri ortaya çıkarılmakta ve bu şekilde suçun nitelikli hali düzenlenirken temel suç tipine bağlı

[769] Akbulut, *Bilişim Alanında Suçlar,* 207.
[770] Dülger, *İnternet İletişim Hukuku*, 357.
[771] Gün, "Bilişim Suçları", 240.; Dülger, *İnternet İletişim Hukuku*, 289.
[772] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1012-1013.; Avşar ve Öngören, *Bilişim Hukuku*, 139.; Çakıcı, "M. 243 ve M. 244'te", 335.

kalınmaya devam edilmektedir[773]. TCK m. 244/4'te yer alan düzenleme TCK m. 244/1-2'deki eylemlerin gerçekleştirilmesi sonucu haksız çıkar sağlanmasını öngördüğünden öncelikle TCK m. 244/1-2'deki hareketlerin gerçekleştirilmesini zorunlu kılmakta; bu şekilde TCK m. 244/1-2'nin devamı niteliği taşımakta ve temel suç tipine bağlılığı devam ettirerek, ilk iki fıkranın nitelikli halini oluşturmaktadır[774]. Buna göre, eylemin başka bir suç oluşturmaması koşulunun asli norm tali norm ilişkisi içinde değerlendirilmesi gerekilmekle birlikte, TCK m. 244'ün özel norm olma niteliğiyle çelişki oluşturmaktadır[775].

İkinci görüşe göre[776], TCK m. 244/4'te yer alan düzenleme, TCK m. 244/1-2'deki suçlarla ihlal şekilleri ve korunan hukuki değerler yönünden farklılık arz eden, kendisinin veya başkasının yararına haksız çıkar sağlama şeklindeki kendi temel şekil unsurları dışında TCK m. 244/1-2'deki unsurları da kapsayacak şekilde oluşturulan ve TCK m. 42'ye göre bileşik suç niteliği taşıyan ayrı bir suçtur[777]. Buna göre ilk iki fıkrada haksız çıkar sağlamanın aranmaması, TCK m. 244/4'ün ağırlaşmış nitelikli hal değil de ayrı bir suç olduğunu ortaya koymaktadır[778]. Diğer bir görüş kanunkoyucunun TCK m. 244/4'ü tali norm şeklinde ve artırım oranı yerine doğrudan ceza belirleyerek TCK m. 244'ü bağımsız suç olarak düzenlediğini gösterdiğini, maddede bir suçta gerekli tüm unsurlara yer verildiğini ifade etmiştir[779]. Yine ayrı bir suç olarak değerlendiren başka bir görüşe göre ise; TCK m. 244/4, TCK m. 244/1-2'den bağımsız, TCK m. 244/1-2'deki eylemleri unsurları olarak içinde barındıran bileşik yapılı[780] ve çok hareketli, tali norm niteliğinde düzenlenen bir suçtur[781]. Bu suçun klasik hırsızlık, dolandırıcılık gibi suçlardan ayrı bir suç olarak düzenlenmesinin nedeni doktrinde bilişim alanında haksız fiilin aslen bir kişiye yöneltilmesi gerekmeden bir sisteme yöneltilerek gerçekleştirilmesi, hedef şahıs faktörünü ortadan kaldırarak kişiye doğrudan temas ile gerçekleştirilen klasik suçlardan ayrılması olarak

[773] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1013.
[774] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1013.
[775] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1014.
[776] Akbulut, *Bilişim Alanında Suçlar,* 217.; Erdoğan, "Engelleme Bozma", 223.; Koca ve Üzülmez, *Özel Hükümler*, 1035.; Dülger, *İnternet İletişim Hukuku*, 365.; Erkan, "Bilişim Sistemine", 93.
[777] Akbulut, *Bilişim Alanında Suçlar,* 217.
[778] Akbulut, *Bilişim Alanında Suçlar,* 217.
[779] Erdoğan, "Engelleme Bozma", 223.
[780] Yaşar, Gökcan ve Artuç, *Yorumlu – Uygulamalı*, 7315.
[781] Koca ve Üzülmez, *Özel Hükümler*, 1035.

gösterilmektedir[782]. Doktrinde ağırlıklı görüşün TCK m. 244/4'te yer alan düzenlemenin ayrı bir suç olduğu yönünde olduğu söylenebilir. Ancak kanaatimce ilk görüşün de ifade ettiği üzere söz konusu düzenleme temel suç tipine bağlılığı devam ettirmekte olduğundan, TCK m. 244/4'ün TCK m. 244/1-2'nin nitelikli halidir.

TCK m. 244/4'te yer alan "*başka bir suç oluşturmaması*" ifadesiyle, eylemin başka bir suç oluşturması durumunda bu fıkranın uygulanmayacağı ifade edilmiş olsa da; gerekçede yer alan "*daha ağır bir cezayı gerektiren başka bir suç oluşturmaması"* ifadesinin düzenlemeyle çelişkiye neden olması ve maddenin yorumlanmasını zorlaştırması sebebiyle doktrinde eleştirilmektedir[783]. Madde metninin belirleyici ve bağlayıcı olması dikkate alınarak, gerekçenin maddenin çelişkisi dolayısıyla, gerekçeye değil madde metnine bağlı kalınmak suretiyle diğer suçun ceza ağırlığına bakılmaksızın eylemin başka bir suç oluşturup oluşturmadığına bakılmalı, oluşturuyorsa TCK m. 244/4'ten ceza verilmemeli, ilgili diğer suçtan hüküm kurulmalıdır[784].

765 sayılı TCK döneminde m. 525/b-2'de; "*Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve iki milyon liradan yirmi milyon liraya kadar ağır para cezası verilir.*" şeklinde düzenlenmişti. Doktrinde bu suç çok geniş bir biçimde düzenlenmiş olması yönüyle eleştirilmiş ve uygulamada zorluklara sebep olmuştu[785]. Bu sebeple, 5237 sayılı kanunda, bilişim sisteminin çalışmasına etki eden hareketleri birbirinden ayırarak, verilere müdahale oluşturan ve suç teşkil eden eylemleri haksız çıkar sağlamanın unsuru haline getirmiş ve bu şekilde sınırlandırmakla birlikte[786], ayrıca; banka ve kredi kartlarını kötüye kullanmak, bilişim sistemleri aracılığıyla hırsızlık ve bilişim sistemleri arayıcılığıyla dolandırıcılık olmak üzere ayrı suç tipleri olarak düzenlendiği ifade edilmiştir[787].

TCK m. 244'de yer alan eylemin ayrı bir suç mu olduğu yoksa nitelikli hal mi olduğu ayrımının önemli sonuçlar doğurduğunu söylemek mümkündür. Bu düzenlemenin nitelikli hal olarak kabulü halinde temel suç işlenmediği sürece bu fıkra

[782] Lal, "Yarar Sağlama", 18.
[783] Dülger, *İnternet İletişim Hukuku*, 365.
[784] Lal, "Yarar Sağlama", 19.
[785] Dülger, *İnternet İletişim Hukuku*, 364.
[786] Akbulut, *Bilişim Alanında Suçlar,* 219.
[787] Dülger, *İnternet İletişim Hukuku*, 364.

uygulanamayacak ve nitelikli hal gerçekleşmediği sürece bu nitelikli hale teşebbüs söz konusu olamayacaktır[788]. Bağımsız suç olduğunu savunan görüşe göre ise; fail eylemi gerçekleştirirken haksız yarar sağlamak kastıyla hareket ettiği halde amacına ulaşamaz ise TCK m. 244/1-2'den değil, TCK m. 244'e teşebbüsten dolayı sorumlu olacaktır[789].

2.3.2. Suçun Manevi Unsuru

765 sayılı TCK döneminde bu suçların düzenlendiği m. 525/b-1'de failin eylemi gerçekleştirirken zarar verme ya da yarar sağlama kastıyla hareket etmesi aranmaktaydı[790]. 5237 sayılı TCK m. 244/1-2'de düzenlenen suçlar ise kasten yani bilerek ve isteyerek işlenebilen suçlar olup failin olası kastı da suçun oluşması için yeterlidir[791]. Eylemin taksirle gerçekleştirilmesi halinde ise taksire ilişkin bir düzenlemeye yer verilmediğinden bu suç oluşmaz[792]. Her ne kadar failin belli bir saikle hareket etmesi aranmasa da birinci ile ikinci fıkranın ayrımı açısından önem taşımakta olup, verilere ilişkin hareketlerle sistemin işleyişinin engellenmesi ya da bozulması gibi hallerde failin hangi fıkraya göre cezalandırılacağının tespitinde failin saiki dikkate alınır[793].

Kastın söz konusu olabilmesi için suçların kanuni tanımında yer alan ve failce gerçekleştirilen sistemin işleyişinin engellenmesi, bozulması, sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi eylemlerinin failce bilinmesi gerekmekte olup, ayrıca gerçekleşme ihtimalini bilmesi de yeterlidir[794]. TCK m. 30'da yer alan hataya ilişkin durumlarda ise, örneğin; failin kendi verileri zannederek başkasının verilerine müdahale etmesi durumunda fail bu hatasından yararlanacak ve böyle bir durumda kastı ortadan kaldıran tipiklik hatası söz konusu olacak, bununla beraber; kullanım hakkını devretmiş malikin, sadece başkasına ait sistemlerdeki verilerin silinmesinin suç olacağına inanması sebebiyle maliki olduğu sistemde yer alan

[788] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1013.
[789] Lal, "Yarar Sağlama", 13.
[790] Akbulut, *Bilişim Alanında Suçlar,* 203.
[791] Akbulut, *Bilişim Alanında Suçlar,* 203.; Koca ve Üzülmez, *Özel Hükümler*, 1031.
Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1019.
[792] Öndin, "Türk Hukukunda", 55.
[793] Dülger, *İnternet İletişim Hukuku*, 357.
[794] Akbulut, *Bilişim Alanında Suçlar,* 203.

kullanıcının verilerini silmesi halinde kastı ortadan kaldıran hata değil, yasak hatası söz konusu olacaktır[795].

Doktrinde devlet kurumlarındaki sistem güvenliğinin ve veri gizliliğinin sağlanmasının önemi vurgulanarak, bu kurumlarda çalışan ve sisteme erişim yetkisi bulunan kişilerin taksirli hareketlerinden dolayı da sorumlu tutulmaları gerektiği ve buna ilişkin bir düzenleme getirilmesinin yerinde olacağı, bu durumda söz konusu kamu görevlisi ya da yetkili kişi bakımından TCK m. 257'de yer alan Görevi Kötüye Kullanma suçunun söz konusu olabileceği düşünülse de yaptırımının konunun önemi dolayısıyla yeterli kalmayacağı ifade edilmektedir[796].

2.3.3. Suçun Hukuka Aykırılık Unsuru

TCK m. 244/1-2'de yer alan suçun gerçekleşebilmesi için eylemin hukuka aykırı olması gerekmektedir. Bunun içinde eylemin icrasında hukuka uygunluk nedenlerinden birinin bulunmaması gerekir.

Bir bilişim sisteminin işleyişinin engellenmesi veya bozulması, sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesinde failin eylemine konu bilişim sistemi ya da veri ilgilisinin rızası hukuka uygunluk nedenini oluşturur[797]. Ancak verilen rızanın sınırlarının aşılması durumunda eylem hukuka aykırı hale gelecektir. Rızayı aşan durumların halinde söz konusu suç oluşacağından rızanın kapsamının net bir biçimde tespit edilmesi gerekir[798].

Yine görevin ifası/ Kanun hükmünün icrası kapsamında icra edilen eylemler de de hukuka uygunluk söz konusudur[799]. Bu kapsamda, örneğin; CMK m. 134 çerçevesinde kolluk güçlerinin delil elde etmeye yönelik gerçekleştirdikleri eylemler[800] ile 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen

[795] Akbulut, *Bilişim Alanında Suçlar,* 204.
[796] Erkan, "Bilişim Sistemine", 153.
[797] Akbulut, *Bilişim Alanında Suçlar,* 204.; Koca ve Üzülmez, *Özel Hükümler,* 1032.
[798] Yılmaz, "5237 Sayılı", 79.
[799] Koca ve Üzülmez, *Özel Hükümler*, 1032.
[800] Dülger, *İnternet İletişim Hukuku*, 358.; Koca ve Üzülmez, *Özel Hükümler*, 1032.

Suçlarla Mücadele Edilmesi Hakkında Kanun" kapsamında erişimin engellenmesi eylemi hukuka uygun olacaktır[801].

Meşru savunmanın bu suçlarda mümkün olup olmadığı konusunda öğretide bir görüş, saldırgana karşı saldırıyı engellemeye yönelik hukuka uygun karşı saldırı ile meşru savunmanın mümkün olduğunu; diğer görüş ise somut olayın özelliklerine göre[802], saldırının niteliğine bakılması gerektiğini, saldırı ağ üzerinden yapılıyorsa ağ bağlantısı kesildiğinde karşı saldırı zorunluluğu kalmadığından meşru savunmanın mümkün olmayacağını, ancak fiilen temasla saldırı yapılıyor ve diğer şartları da varsa meşru savunmanın mümkün olduğunu ifade etmektedir[803].

Zilyedin ya da malikin güvenlik amacıyla -örneğin üretici firmaca dışardan gelen saldırılardan korumak amacıyla öngörülenin dışında eylemler gerçekleştirilmesi halinde sisteme de zarar verici çeşitli tuzak yazılımlar yerleştirmesi gibi- bir takım tedbirler alması ve bu yolla saldırganın verilerine ve/veya bununla birlikte sisteme zarar vermesi halinde korunan hukuki yararla zarar arasında orantı varsa sisteme zarar verme davranışı hukuka uygun kabul edilebilir[804].

2.4. Suçun Özel Görünüş Biçimleri

2.4.1. Teşebbüs

TCK m. 244 kapsamında düzenlenen tüm suçlara teşebbüs mümkündür. Bu suçlarda teşebbüs, hareketlerin icrasına başlandıktan sonra eylemin yarıda kalması şeklinde gerçekleşebileceği gibi; suçun icrasına dair tüm hareketler gerçekleştirildikten sonra suçun oluşumunda aranan neticenin meydana gelmesinden önce, failin elinde olmayan sebeplerle suçun gerçekleşememesi şeklinde de olabilir[805]. Örneğin, fail tarafından sisteme yüklenen zararlı bir yazılımın aktive edilemeden önce sistem sahibi tarafından veyahut virüs programları tarafından fark edilerek ortadan kaldırılması halinde suça teşebbüs söz konusudur. Teşebbüsün mümkün olması dolayısıyla failin fiilin icrasına

[801] Uçar, "Bilişim Suçları", 68.; Koca ve Üzülmez, *Özel Hükümler*, 1030.; Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1018.
[802] Geçmez, *Değiştirme Suçları,* 99.
[803] Erdoğan, "Engelleme Bozma", 164.
[804] Demircan, *Bilişim Alanında Suçlar,* 90. Yazıcıoğlu, *Bilgisayar Suçları*, 257.
[805] Dülger, *İnternet İletişim Hukuku*, 359.; Erdoğan, "Engelleme, Bozma", 169.

başladıktan sonra pişman olarak gönüllü vazgeçmesi de mümkündür, ancak bu durumda vazgeçme anına kadar tamamlanmış bir suçu varsa bundan dolayı sorumlu olacaktır[806]. Örneğin; failin sistemdeki verileri başka bir yere göndermek amacıyla sisteme girmesi ancak daha sonrasında verileri başka bir yere göndermekten vazgeçmesi halinde TCK m. 36'da düzenlenen gönüllü vazgeçme gerçekleşecek, böylece fail TCK m. 244/2'ye teşebbüsten sorumlu olmamakla beraber; tamamlanmış suç olan TCK m. 243/1'den sorumlu olacaktır[807].

TCK m. 244/1-2'deki suçlar seçimlik olarak düzenlendiğinden herhangi birisi gerçekleştirildiği takdirde diğer seçimlik belirlemeler teşebbüs aşamasında kalsa dahi suç tamamlanmış sayılır[808]. Yani, failin seçimlik hareketlerden birkaçını gerçekleştirmiş olması halinde, bu hareketlerden bir kısmı tamamlanmış ancak diğer bir kısmı teşebbüs aşamasında kalmış olsa dahi, suç tamamlanmış sayılır ve faile tamamlanmış suçun cezası verilir[809]. Örneğin; failin sistemdeki verileri başka sisteme aktarmayı ve aynı zamanda sistemdeki söz konusu verileri değiştirerek farklı veriler eklemeyi planlaması halinde, fail var olan verileri başka yere göndermiş ancak sisteme veri yerleştiremeden sistemden atılmışsa suç gerçekleşmiş olur ve faile tamamlanmış suçun cezası verilir.

2.4.2. Suça İştirak

TCK m. 244'de düzenlenen suçlarda iştirak yönünden herhangi bir özel düzenleme getirilmemiş olup bu suçlara TCK'da iştirake ilişkin düzenlenen genel hükümler uygulanır.

2.4.3. Suçların İçtiması

Ceza hukukunda tipe uygun eylem yani hareket ile suç tipince korunan hukuki menfaat olmak üzere iki temel bulunmakta olup, buna göre; belli bir hukuki menfaati koruyan kaç hareket ya da eylem varsa o kadar suçun oluştuğu kabul edilmesine gerçek içtima denir[810]. Failin tek fiilliyle birden fazla farklı suçun oluşması durumunda ise (farklı

[806] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1019.
[807] Öndin, "Türk Hukukunda", 64.; Taşkın, "Karşılaştırmalı Hukukta, 64.; Mehmet Emin Artuk, Ahmet Gökçen ve A. Caner Yenidünya, Ceza Hukuku Özel Hükümler, (Ankara: Adalet Yayınevi, 2015), 889.
[808] Akbulut, *Bilişim Alanında Suçlar,* 209.
[809] Dülger, *İnternet İletişim Hukuku*, 359.
[810] Veli Özer Özbek vd., *Türk Ceza Hukuku Genel Hükümler*, (Ankara: Seçkin Yayınları, 2023), 565.

neviden) fikri içtima söz konusu olur ve böyle bir durumda fail en ağır cezayı gerektiren suçu işlemiş kabul edilir[811]. Failin bir suçu işleyebilmek için başka bir suçu da işlemesinin zorunlu olduğu suçlara ise (tüketen-tüketilen norm ilişkisi)[812] geçitli suçlar denmekte olup[813] bu tarz suçlarda daha ağır eylem daha hafif eylemi içine alır ve bu durumda fail daha ağır olan suçtan cezalandırılır[814].

Yukarıdaki açıklamalar ışığında; bir bilişim sistemine girilerek TCK m. 244/2'de yer alan verilerin bozulması veya TCK m. 244/1'de yer alan sistemin engellenmesi eylemlerinin gerçekleştirilmesi halinde TCK m. 243 ile TCK m. 244 bakımından nasıl bir ilişki kurulacak ve fail nasıl cezalandırılacaktır? Doktrinde failin TCK m. 243'te yer alan bilişim sistemine girme suçu ile TCK m. 244'te yer alan suçları birlikte işlemesi halinde bir görüşe göre fikri içtima uygulanması gerekirken[815], bir görüş bu suçların geçitli suç olduğunu[816], bir görüş failin kastına göre belirleme yapılması gerektiğini[817], başka bir görüş ise gerçek içtima uygulanması gerektiğini savunmaktadır[818]. Yine bu konuda diğer bir görüşe göre ise burada geçit suç olup olmadığı suç tipindeki her hareket ve somut olayın özellikleri değerlendirilerek belirlenecektir[819]. Yargıtay ise TCK m. 243 ile TCK m. 244/2'nin birlikte gerçekleştiği hallerde TCK m. 244'ten cezalandırılma yapılması gerektiği kanaatindedir[820]. Yine doktrinde bir görüşe göre bilişim sistemine orada kalmak maksadıyla girip sonradan kastını değiştirerek TCK m.

---

[811] Özbek vd., *Genel Hükümler*, 583.
[812] Yılmaz, "5237 Sayılı", 83.
[813] Erkan Sarıtaş, "Cezalandırılmayan Önceki Hareketler", *İstanbul Hukuk Mecmuası*, 80/2 (2022): 645. 10.26650/mecmua.2022.80.2.0008 https://dergipark.org.tr/pub/ihm http://mecmua.istanbul.edu.tr/tr/_
[814] Demircan, *Bilişim Alanında Suçlar,* 106. Ahmet Taşkın ve İbrahim Zengin, *Ceza Hukuku El Kitabı*, (Ankara: Seçkin Yayıncılık, 2004), 43.
[815] Koca ve Üzülmez, *Özel Hükümler,* 1033.; Akbulut, *Bilişim Alanında Suçlar,* 212.; Apaydın, *Bilişim Sistemine*, 182.; Geçmez, *Değiştirme Suçları,* 104.; Erdoğan, "Engelleme Bozma", 172.
[816] Yılmaz, "5237 Sayılı", 83.; Erdoğan, "Engelleme Bozma", 171.; Bük, *Verilerin Korunması,* 125.; Gül, *Doğrudan Dolaylı,* 140.; Mahmutoğlu, "Yargı Kararları Işığında", 869.; Artuk, Gökçen ve Yenidünya, *Özel Hükümler*, 878.; Artuk, Gökçen ve Yenidünya, *Ceza Kanunu,* 4664.
[817] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1000.
[818] İsmail Malkoç, *Açıklamalı – İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu Madde 179-345 2. Cilt*, (Ankara: Malkoç Kitabevi Yayınları, 2008), 2070.
[819] Dülger, *İnternet İletişim Hukuku*, 362.
[820] Yargıtay'ın TCK 243 ile 244'ün birlikte gerçekleşmesi halinde TCK 244'ten hüküm kurulması gerektiğine ilişkin kararı şu şekildedir:"*…bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme ile bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, var olan verileri başka bir yere gönderme suçlarına ilişkin olarak, sanığın, yetkisi olmadığı halde katılan şirkete ait bilişim sistemine girerek orada bulunan verileri alıp kendi kullandığı bilgisayara ve CD'ye aktarması şeklinde gerçekleşen eyleminin bir bütün olarak TCK.nun 244/2. maddesinde düzenlenen suçu oluşturacağı gözetilmeden yazılı şekilde karar verilmesi...*"; Yargıtay 8. Ceza Dairesi, 14.07.2014, E. 2013/3173, K. 2014/ 18506, https://kararara ma.yargitay.gov.tr/ E.T. 15.01.2025.; Gün, "Bilişim Suçları", 248.

244/2'deki eylemlerden birini gerçekleştirmişse bu durumda eklenen kast nedeniyle TCK m. 244/2 uyarınca cezalandırılacaktır[821]. Buna karşın başka bir görüş zamansal yakınlık değerlendirmesi yapılması gerektiğini, zamansal yakınlık yoksa failin farklı kastla eylemde bulunduğunun kabulü halinde her iki suçtan ayrı ceza verilmesi gerektiğini ifade etmektedir[822]. Bu konuda TCK m. 244 açısından sisteme girme zaruri bir eylem olmadığından, somut olayın özelliklerine göre değerlendirilerek, tek fiille her iki suç tipinin ihlalinin söz konusu olması halinde fikri içtima yapılması gerektiği ifade edilmelidir.

TCK m. 244'te yer alan suçlarda aynı fıkra kapsamındaki hareketlerden birkaçının aynı olayda bir arada icra edilmesi halinde birden fazla suç oluşmaz, faile tek ceza verilir[823]. Örneğin; failin bir sistemde yer alan verilerin bir kısmını bozması, diğer bir kısmının ise erişilmez kılınması halinde tek bir cezaya hükmolunacaktır.

TCK m. 245/A'da yer alan suç ile TCK m. 244'de yer alan suçun beraber işlenmesi durumunda ise; TCK m. 245/A'da yer alan yasak cihaz ve programların imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması suçu ile hazırlık hareketlerine yönelik eylemler ayrı ve bağımsız bir suç olarak düzenlendiğinden TCK m. 244'te yer alan suçlarla beraber işlenmesi durumunda gerçek içtima söz konusu olacaktır[824].

Failin tek eylemiyle hem TCK m. 244/2 hem de TCK m. 267 ve TCK m. 271'de yer alan suçları beraber işlemiş olması halinde, bu durumda, farklı neviden fikri içtima uygulanması suretiyle faile en ağır suçtan ceza verilmesi gerekecektir[825]. Örneğin; failin bir sisteme veri yerleştirmek suretiyle başka bir kişinin suç işlediği görünümü vermesi durumunda hem TCK m. 244/2 hem de TCK m. 267 ve TCK m. 271'de yer alan suçlar işlemiş olacak ve fikri içtima uygulanarak faile en ağır suçun cezası verilecektir.

[821] Gül, *Doğrudan Dolaylı*, 140.
[822] Dülger, *İnternet İletişim Hukuku*, 318.
[823] Demircan, *Bilişim Alanında Suçlar,* 105.; Dülger, *İnternet İletişim Hukuku*, 359.
[824] Akbulut, *Bilişim Alanında Suçlar,* 212.
[825] Dülger, *İnternet İletişim Hukuku*, 361.

Aynı suç işleme kararı kapsamında farklı zamanlarda aynı kişiye karşı aynı suçun birden fazla kez işlenmesine ise zincirleme suç denir[826]. TCK m. 244/1-2'de yer alan suçlar zincirleme suç şeklinde işlenebilir. Ancak burada zincirleme suç hükümlerinin uygulanabilmesi için aynı suçun ihlal edilmiş olması gerekmekte olup, farklı hukuki değerleri koruyan suçların bir arada işlenmesi halinde, örneğin; TCK m. 244/1 ile TCK m. 244/2'nin peş peşe ihlal edilmesi halinde, zincirleme suç hükümleri uygulanmaz[827]. Yani burada kastedilen aynı kanun maddesinin birden fazla kez ihlali değil, aynı suçun birden fazla kez işlenmesi halidir[828]. Örnek olarak; aynı suç işleme kastıyla sistemin çalışmasını engellemek için kısa zaman aralıklarıyla sisteme birden fazla kez saldırı düzenlenmesi halinde zincirleme suç söz konusu olur[829]. Aynı suç işleme kararı kapsamında görülemeyecek kadar uzun aralıklarla ya da farklı eylemlerle, farklı amaçlarla gerçekleştirilen eylemler varsa faile her eylemden dolayı ayrı ceza verilecektir[830]. Bununla birlikte, Yargıtay 12. Ceza Dairesi bir kararında iki farklı bilişim sistemi için de zincirleme suç hükümlerinin uygulanmasına karar vererek; e-posta hesabı ile facebook hesabını iki farklı bilişim sistemi olarak kabul etmiş ve aynı mağdura karşı aynı suç işleme kararı çerçevesinde gerçekleştirilen eylemlere yönelik olarak zincirleme suç hükümlerinin uygulanmasına karar vermiştir[831].

TCK m. 244/1 ve TCK m. 244/2'deki suçların her ikisinin birlikte gerçekleştirilmesi halinde (örneğin; sistemdeki verilerin bozulmasının ve sistemin bozulmasının birlikte gerçekleştirilmesi gibi) doktrinde bir görüşe göre, tek fiille farklı suçlar gerçekleştiğinden fikri içtima uygulanarak sorunun çözümlenmesi gerekirken[832]; ikinci görüşe göre TCK m. 244/2'deki hareketler TCK m. 244/1'e vücut verdiyse burada TCK m. 244/1'deki suç oluşacak ve faile 244/1 kapsamında ceza verilecektir[833]. Kanaatimce bu durumda failin saikine bakılması gerekmektedir. Failin TCK m. 244/2'deki eylemleri gerçekleştirmekteki kastı TCK m. 244/1'e yönelikse, bu durumda fikri içtima

[826] Özbek vd., *Genel Hükümler*, 570.
[827] Dülger, *İnternet İletişim Hukuku*, 360.
[828] Özbek vd., *Genel Hükümler*, 571.
[829] Dülger, *İnternet İletişim Hukuku*, 360.
[830] Öndin, "Türk Hukukunda", 57.
[831] Yargıtay 12. Ceza Dairesi 01.03.2017, E. 2015/10388, K. 2017/1556, https://kazanci.com.tr/, E.T. 15.01.2025.; Dülger, *İnternet İletişim Hukuku*, 360.
[832] Erdoğan, "Engelleme Bozma", 215.; Bük, *Verilerin Korunması*, 120.; Geçmez, *Değiştirme Suçları*, 105.
[833] Koca ve Üzülmez, *Özel Hükümler*, 1030.

uygulanarak sorunun çözülmesi gerekmektedir. Ancak TCK m. 244/1'e yönelik olası kastı dahi yoksa bu durumda TCK m. 244/2 kapsamında değerlendirilmesi gerekmektedir.

Tek fiille aynı suçun birden fazla kişiye karşı işlenmesi haline ise aynı neviden fikri içtima denir[834] ve bu durumda zincirleme suç hükümleri uygulanır. Buna göre; bir zararlı yazılım içeren programın internette yayımlanması ve bunu indiren birçok kişinin sistemine bulaşması halinde, aynı suçun birden fazla kişiye karşı tek hareketle işlenmesi söz konusu olduğundan aynı neviden fikri içtima uygulanacaktır[835]. Yine başka bir örnekle, failin aynı spam mailini tek seferde birden çok kişiye göndererek sistemlerine virüs bulaştırması gibi bir eylemde bulunması halinde de TCK m. 43/2 söz konusu olacaktır[836].

TCK m. 244/4'teki düzenlemeye yönelik olarak, TCK m. 244/4'ü ayrı suç olarak değerlendiren görüşe göre TCK m. 244/1-2'deki suçlar ile TCK m. 244/4'te yer alan suçun arasında fiil tekliği ilişkisi bulunmakta olup, ilk iki fıkradaki hareketler TCK m. 244'ün unsuru niteliğinde olduğundan; failin sisteme veya verilere müdahale ederek çıkar sağlaması durumunda, fail yalnızca TCK m. 244/4 kapsamında cezalandırılacaktır[837].

TCK m. 244/2'de yer alan verilere müdahale ile TCK m. 151'de yer alan mala zarar verme suçu arasındaki ilişki ise farklı durumlara göre değişkenlik göstermektedir. Failin başkasının sistemine zarar verirken verilere de zarar vermesi gibi bir durumda doktrinde bir görüşe göre hem mala zarar verme hem de verilere müdahale suçunu ihlal etmiş olacağından fikri içtima yapılması gerekirken; kendi bilişim sistemine zarar vermek suretiyle başkasının verilerine zarar vermişse fail yalnız TCK m. 244'ten sorumlu olacaktır[838]. Failin tek fiille hem TCK m. 151'de yer alan mala zarar verme hem de TCK m. 244/2'de yer alan verilere müdahale suçunu ihlal etmiş olması durumuna ilişkin diğer bir görüşe göre ise bu iki madde aynı suçu düzenlemekte olup TCK m. 244 özel bir nas'ı ızrar suçu olduğundan, burada genel düzenlemeye göre özel düzenlemenin

[834] Özbek vd., *Genel Hükümler*, 580.
[835] Dülger, *İnternet İletişim Hukuku*, 361.
[836] Öndin, "Türk Hukukunda", 57.; Dülger, *İnternet İletişim Hukuku*, 361.
[837] Akbulut, *Bilişim Alanında Suçlar,* 210.; Koca ve Üzülmez, *Özel Hükümler*, 1033.
[838] Akbulut, *Bilişim Alanında Suçlar,* 210.

uygulanmasını gerektiren kuralların dikkate alınması gerekmektedir[839]. Buna karşın başka bir görüş ise korunan hukuki değerler farklı olduğundan iki madde arasında özel hüküm genel hüküm ilişkisi bulunmadığını, yani bir diğer ifadeyle; TCK m. 244'ün özel bir nas-ı ısrar suçu olmadığını ifade etmektedir[840]. Ayrıca yine bu görüşe göre TCK m. 244'ün gerekçesinde sırf "ızrar" yazıyor diye sadece mala zarar verme kastıyla gerçekleştirilen eyleme TCK m. 244'ün uygulanmaması gerekmektedir[841]. Bununla birlikte başka bir görüş burada TCK m. 244 ve TCK m. 151 arasında failin kastının hangi suça yönelik olduğunun belirlenmesi gerektiğini ve buna göre cezalandırma yapılması gerektiğini ifade etmektedir[842].

Failin TCK m. 142/1-e veya TCK m. 158/1-f ile birlikte TCK 244/4'ü ihlal etmesi halinde: TCK m. 244/4'te eylemin başka bir suç oluşturmaması halinde bu fıkranın uygulanacağı düzenlendiğinden eylemin TCK m. 142/1-e veya TCK m. 158/1-f kapsamında olması halinde TCK m. 244/4'ten değil, bu suçlardan hüküm kurulacaktır. Failin verilere müdahale ederek sahte belge düzenlemesi halindeyse bir görüşe göre fikri içtima uygulanarak en ağır cezayı gerektiren suçtan sorumlu olması gerekirken[843], diğer görüşe göre gerçek içtima uygulanması gerekmektedir[844]. Bu konuda bir görüşe göre her somut olayın kendi içinde değerlendirilmesi gerekmekte olup, örnek olarak sahte belge kullanmak suretiyle sisteme giriş izni sağlandıktan sonra TCK m. 244/2'deki eylemlerin gerçekleştirilmesi halinde iki ayrı suçtan hüküm kurulması gerekirken verilere müdahale ile sahte belge düzenlenmesi durumunda fikri içtima yapılması gerekmektedir[845]. Yargıtay Ceza Genel Kurulu'nun kararına göre ise; elektronik belgede sahtecilik eylemlerine ilişkin olarak gerçekleşen olayda, özel normun önceliği ilkesi gereği, belgede sahtecilik suçunun yer aldığı TCK m. 204/1 değil, özel norm vasfında olan TCK m. 244/2'nin uygulanması gerekmektedir[846].

---

[839] Mahmutoğlu, "Yargı Kararları Işığında", 866.; Demircan, *Bilişim Alanında Suçlar,* 108.; Yazıcıoğlu, *Bilgisayar Suçları*, 266.; Demirci, *Soruşturma Yöntemleri*, 98.
[840] Dülger, *İnternet İletişim Hukuku*, 361.
[841] Dülger, *İnternet İletişim Hukuku*, 361.
[842] Erdoğan, "Engelleme Bozma", 176.; Yılmaz, "5237 Sayılı", 82.; Malkoç, *Açıklamalı – İçtihatlı*, 2078.
[843] Akbulut, *Bilişim Alanında Suçlar,* 211.
[844] Artuk, Gökçen ve Yenidünya, *Ceza Kanunu*, 4670. Artuk, Gökçen ve Yenidünya, *Özel Hükümler*, 889.
[845] Erdoğan, "Engelleme Bozma", 216.
[846] Yargıtay'ın TCK 244'ten hüküm kurulması gerektiğine ilişkin kararı şu şekildedir: "…TCK'nın 244. maddesinin ikinci fıkrasındaki bu düzenlemenin elektronik belgelerde yapılacak sahtecilik eylemlerine

TCK m. 244 ile haberleşmenin engellenmesi suçunu düzenleyen TCK m. 124'ün birlikte ihlali halinde fikri içtima uygulanarak daha ağır ceza içeren TCK m. 244'ün uygulanması gerekir[847]. TCK m. 244/4 ile TCK m. 163/1'de yer alan karşılıksız yararlanma suçunun ayrımı noktasında ise "bedeli karşılığı hizmet verilen otomat" ifadesinden ne anlaşılacağı belirleyici olmaktadır[848]. Yargıtay bu konuda ankesörlü telefonları merkezi bilgisayar sistemi ile yönetilen hizmet telefonları olarak değerlendirmekte olup; bir kararında failin kredisi bitmiş manyetik telefon kartlarına hileli yöntemlerle kontör yüklemesini TCK m. 163 değil, TCK m. 244/4 kapsamında değerlendirmiştir[849].

2.5. Muhakeme

2.5.1. Soruşturma ve Kovuşturma

TCK m. 244/1-2'de yer alan suçlar TCK m. 11/2 düzenlemesi hariç olmak üzere şikâyete tabi olmayıp, re'sen takip edilen suçlardır[850]. Bu suçlarda görevli mahkeme 5237 sayılı Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun m. 11'e göre Asliye Ceza Mahkemeleridir. Yetkili mahkeme ise hareketin kısmen veya tamamen işlendiği ya da neticenin gerçekleştiği yer, yani suçun işlendiği yer mahkemesi olup; bu suçlarda failin fiziki olarak bulunduğu yer ile hareketin açığa çıktığı yerler farklı olabileceğinden, hem failin fiziken bulunduğu yer hem de hareketin açığa çıktığı yer hareket yeri olarak kabul edilir[851]. Tüm bu açıklamalarla birlikte, bu davalara, 30.11.2021 tarihli Resmi Gazete'de yayımlanan 1229 sayılı HSK kararı kapsamında bu suçlara ilişkin dava ve işlerin görülmesi için özel olarak belirlenen ihtisas mahkemelerince bakılacağı

---

ilişkin özel norm niteliğinde olduğu ve özel normun önceliği ilkesi gereğince de sanık hakkında genel normun değil özel normun uygulanması gerektiği…"; Yargıtay Ceza Genel Kurulu, 29.09.2020, E. 2017/1122, K. 2020/381, https://kararara ma.yargitay.gov.tr/, E.T. 15.01.2025.: Dülger, *İnternet İletişim Hukuku*, 362.

[847] Erdoğan, "Engelleme Bozma", 173.; Geçmez, *Değiştirme Suçları,*105.

[848] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1052.

[849]Yargıtay Ceza Genel Kurulu, 19.06.2007, E. 2007/6-136, K. 2007/150. https://kararara ma.yargitay.gov.tr/. E.T. 15.01.2025.; Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1052.

[850] Akbulut, *Bilişim Alanında Suçlar,* 215.

[851] Akbulut, *Bilişim Alanında Suçlar,* 216.

düzenlenmiştir[852]. Bu suçlarda dava zamanaşımı süresi ise TCK m. 66/1-e gereğince 8 yıldır[853].

5271 sayılı CMK m. 253/1-c'de "*Mağdurun veya suçtan zarar görenin gerçek veya özel hukuk tüzel kişisi olması koşuluyla, suça sürüklenen çocuklar bakımından ayrıca, üst sınırı üç yılı geçmeyen hapis veya adli para cezasını gerektiren suçlar*" bakımından uzlaşma hükümlerinin uygulanacağı düzenlenmiş olup, bu kapsamda TCK m. 244/2'de yer alan suçun SSÇ tarafından işlenmesi halinde bu suç için uzlaşmaya hükümleri uygulanacaktır[854]. TCK m. 51'e göre ise 18 yaşını doldurmuş 65 yaşını bitirmemiş kişiler bakımından işlediği suçtan dolayı iki yıl veya daha az süreyle hapis; 18 yaşını doldurmamış ve 65 yaşını bitirmiş kişiler bakımından ise üç yıl veya daha az süreyle hapis cezasına mahkûm edilen kişinin cezası ertelenebilir[855].

Bilişim suçları bilişim sistemleri üzerinden gerçekleştirilen ve bunlara karşı işlenen suçlar olup bu suçların tespitinde klasik delillerden çok elektronik deliller etkindir. Bu suçların tespiti büyük çoğunlukla elektronik deliller aracılığıyla gerçekleştirilmekte ve suç failleri yine bu deliller aracılığıyla ortaya çıkarılmaktadır. Ceza yargılamasında kullanılabilecek deliller maddi olayın tamamı ya da bir kısmını yansıtan, olayı ispatlayabilecek ya da çürütebilecek belirtilerdir[856]. Bunların delil olarak kabul edilebilmesi için akılcı, bilimsel, ulaşılabilir olması ve hukuka uygun bir biçimde elde edilmiş olması gerekir[857]. Dijital deliller bilişim sistemi ve depolama aygıtları üzerinden elde edilen adli delillerdir[858]. Bu deliller sayıları esas alan yöntemlerle çalışan elektronik cihazlarda saklanan ve bu cihazlar vasıtasıyla oluşturulan deliller olup elektronik delil kavramının içerisinde yer alır[859]. Dijital delillerin yapısı itibariyle "latent" yani gizli bir yapıda olması nicel bir gözlem yapılmasını ve açığa çıkarılabilmeleri için uygun alet ve cihazlar yardımıyla bir uzman tarafından incelenmesini gerekli kılmaktadır[860]. Bunlar dış dünyaya ancak görsel ya da işitsel olarak yansıtılabilen ve elde edilmesi kolay

[852] Dülger, *İnternet İletişim Hukuku*, 363.
[853] Uçar, "Bilişim Suçları", 70.
[854] Dülger, *İnternet İletişim Hukuku*, 363.
[855] Demircan, *Bilişim Alanında Suçlar,* 109.
[856] Şenel Sarsıkoğlu, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", *Türkiye Adalet Akademisi Dergisi,* 22 (2015): 433.
[857] Sarsıkoğlu, "Ceza Muhakemesinde Delil", 434.
[858]Ayşenur Demiral, "Dijital Delil Nedir? Ne işe Yarar?", (E. T. 02.02.2025), https://www.siberegitmen.com/dijital-delil-nedir/
[859] Sarsıkoğlu, "Ceza Muhakemesinde Delil", 439.
[860]Muharrem Özen ve Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)", *Ankara Barosu Dergisi*, 1 (2015): 59.

olmayan deliller olup genellikle incelenen cihazdan başka kullanılan yardımcı cihazın kapsamı ve ölçüsü dahilinde elde edilmektedir[861]. Elde edilen delil muhafazasında oluşturulan koruma zincirinin bozulması elektronik delilin delil olarak geçerliliğini etkileyeceğinden[862] delilin elde edilmesinin yanında mahkeme huzuruna korumalı bir biçimde çıkarılması da oldukça önem arz etmektedir. Elektronik delillerin inceleme ve analizi sırasında yapılabilecek bir hata zarar görmesine yol açabileceğinden orijinal verilerin kopyasının alınması bir zorunluluk olup bu kopya adli kopya olarak da ifade edilmektedir[863]. Elde edilen bu kopyanın orijinalinin birebiri olması ve üzerinde çalışılan söz konusu delilin bütünlüğü gözetilerek araştırma sürecinde herhangi bir değişikliğe uğramadığını ortaya koyacak teknik ispatın da sağlanması gerekmektedir[864]. Elektronik deliller klasik delillere göre kendine has farklı özellikler taşısa da bir delil türü olmayıp delil şekli olduğundan[865], bilimsel yöntemlere uyulmak suretiyle ve hukuka uygun bir biçimde elde edildikleri takdirde ceza yargılamasında tek başına delil olarak kullanılması da mümkündür. Burada önemli olan doğru yöntemlerle elde edilen delilin sonuç itibariyle yargıyı işlenen suç ile eylemi gerçekleştiren faile ulaştırması ve bu yöndeki ispat kabiliyetidir.

2.5.2. Yaptırım

TCK m. 244/1'de bir bilişim sisteminin işleyişini engelleyen veya bozan kişiye bir yıldan 5 yıla kadar, TCK m. 244/2'de ise bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişiye altı aydan 3 yıla kadar hapis cezası öngörülmüştür. Görüldüğü üzere her iki suç için de kanunda yalnızca hürriyeti bağlayıcı ceza öngörülmüş olup adli para cezasına yer verilmemiştir. Doktrinde ise bu suçlar yönünden 576 sayılı TCK'da m. 525/b-1'de düzenlendiği gibi hem hürriyeti bağlayıcı ceza hem de adli para cezasının düzenlenmesinin ve -benzer nitelikte olan mala zarar verme suçunda da düzenlemenin bu şekilde yapılmış olması da dikkate alınarak- seçimlik bir ceza öngörülmesinin çok

[861]Yusuf Başlar, "Elektronik Delilin Toplanması ve Muhafazası", *Hacettepe Hukuk Fakültesi Dergisi*, 10/1 (2020): 80.
[862]Başlar, "Elektronik Delilin", 81.
[863]Başlar, "Elektronik Delilin", 90.
[864]Başlar, "Elektronik Delilin", 92.
[865] Sarsıkoğlu, "Ceza Muhakemesinde Delil", 443.

daha yerinde olacağını ifade edilmiştir[866]. Ancak, TCK m. 49/2 uyarınca TCK m. 244/1 ve 2'deki suçların alt sınırının kısa süreli kabul edilmesi dolayısıyla, alt sınırdan ceza verilmesi halinde cezanın TCK m. 50/1'de düzenlenen seçenek yaptırımlara çevrilmesi olanağı bulunmaktadır.

TCK'da sistemin işleyişi, sistemde yer alan verilerden daha önemli görülerek TCK m. 244/1'de yer alan sisteme ilişkin fiillere TCK m. 244/2'de yer alan verilere müdahale eylemlerinden daha ağır nitelikte ceza öngörülmüştür[867]. Ancak doktrinde, verilerin bilişim sisteminden daha değerli olabileceği haller olduğunu, bu sebeple verilerin bilişim sisteminden daha değerli olması halinde faile verilecek cezanın arttırılmasını öngörecek nitelikte bir düzenlemenin yapılmasının yerinde olacağı ifade edilmiştir[868]. Başka bir görüşte iki fıkra arasında ceza farkının uygulamada soruna yol açtığını, ayrıca failin fiş çekerek TCK m. 244/1 kapsamında sisteme erişimi engellenmesi halinin özel yetenek gerektiren yöntemlerle TCK m. 244/2'deki verilere erişimi engellemesi halinden daha fazla ceza alacak olmasının suç siyasetiyle bağdaşmadığı ifade edilmektedir[869]. Yine; düzenlenen cezanın tür ve miktarı ne olursa olsun hem suçların niteliği hem de takibine ilişkin sorunlar bakımından, mevcut düzenlemenin suçların önlenmesinde yeterli olmadığı ve bu suçların işlenme sıklığı ile ortaya çıkardığı zararın ağırlığı dikkate alındığında da cezanın alt sınırının oldukça düşük kaldığı ifade edilmektedir[870]. Bilişim suçlarının işlenmesinde sürekli yeni yöntemler ortaya çıkarılması dolayısıyla tehlikenin günden güne arttığı, bu tehlike sebebiyle kişilere korunmaya yönelik herhangi bir zorunluluk getirilemeyeceğinden, korumanın yasal düzenlemeyle sağlanması ve yaptırımların ağırlaştırılması gerektiği ve bu kapsamda suçun alt ve üst sınırının yukarı çekilmesinin yerinde olacağı ifade edilmektedir[871]. Bu konudaki görüşlerin isabetli olduğu ifade edilmelidir. Bilişim suçlarının ortaya çıkardığı tehlikenin boyutu göz önünde bulundurulduğunda cezalar oldukça hafif kaldığından ceza hukukunun caydırıcılık fonksiyonunu sağlamaktan uzaktır. Özellikle işlenmesindeki kolaylık ve anonim bir biçimde hareket serbestisi sağlayan yapısı, bu suçlarla mücadelede büyük zorluklar çıkarırken, caydırıcılık etkisi göstermeyecek

[866] Akbulut, *Bilişim Alanında Suçlar,* 213.
[867] Dülger, *İnternet İletişim Hukuku*, 362.
[868] Karagülmez*, Bilişim Suçları,* 246.
[869]Yazıcıoğlu, "Yeni Türk", 117.
[870] Akbulut, *Bilişim Alanında Suçlar,* 214.; Koca ve Üzülmez, *Özel Hükümler*, 1034.
[871] Erkan, "Bilişim Sistemine", 154.

derecede düşük seviye yaptırımların uygulanması potansiyel failler üzerinde gerçekçi bir etki uyandırmamaktadır. Eylemin yöneldiği tehlikenin boyutuna göre katmanlı bir yaptırım şekli düzenlenmesinde fayda vardır. Bu da hem temel cezanın üst sınırlarının artırılması, hem de risk oluşturduğu tehlikenin boyutlarına göre farklı nitelikli haller ve neticesi sebebiyle ağırlaşmış haller düzenlenmek sureti ile sağlanmalıdır.

TCK m. 244/3'te ise bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali suçun nitelikli hali olarak düzenlenmiş olup, söz konusu düzenlemeyle bu tarz bir durumda TCK m. 244/1 ve TCK m. 244/2'ye göre verilecek cezanın TCK m. 244/3 kapsamında yarı oranında arttırılacağı belirtilmiştir. TCK m. 246'da ise bu suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenleme altına alınmıştır.

2.6.Benzer Suç Tipleriyle Karşılaştırılması

2.6.1. Mala Zarar Verme ile Karşılaştırılması

Mala zarar verme suçunda suçun konusu başkasına ait taşınır veya taşınmaz bir mal olup, mal tabirinden, az da olsa maddi veya manevi bir değere sahip; katı, sıvı, gaz halde olması önem taşımadan bir yer işgal eden bütün maddeler anlaşılır[872]. Bu suçla korunan hukuki değer ise bir kimseye bir şey üzerinde kullanma, yararlanma ve tüketme yetkisi veren mülkiyet hakkıdır[873].

Hukuki anlamıyla mal, hukuk düzeninin mülkiyet hakkı tanıdığı maddi eşyalar olup güneş ışığı, hava veya enerji gibi somut olmayan varlıklar, medeni hukukun mülkiyete konu ettiği fikri eserler ile bilişim verileri gibi soyut unsurlar maddi bir yapıları olmadığından eşya sayılamazlar ve mala zarar verme suçunun kapsamına girmezler[874]. Dolayısıyla sistem verileri ve diğer bilişim verileri hukuken mal vasfında görülmediğinden dolayı bunlara yönelik yapılan zarar verici eylemler mala zarar verme suçu kapsamında değerlendirilememiş ve daha önce de belirttiğimiz üzere gerek Türkiye gerekse diğer devletlerce yeni düzenleme yapılması yoluna gidilerek bunlara

[872] Atilla Geyik, "Türk Ceza Hukuku'nda Mala Zarar Verme Suçu", (Yüksek Lisans Tezi, Dicle Üniversitesi, 2014), 29.
[873] Emre Polat, "Yargı Kararları Işığında Mala Zarar Verme Suçu", (Yüksek Lisans Tezi, Selçuk Üniversitesi, 2023), 30.
[874] Polat, "Mala Zarar", 41-43.

yönelik koruma sağlanmaya çalışılmıştır. Bununla birlikte doktrinde de TCK m. 244'te yer alan suçlar ile mala zarar verme suçları arasında bir bağlantının bulunduğu yönünde birçok görüş olduğu ve bilişim suçları açıklanırken çoğu zaman mala zarar verme suçu ile ilişkisi üzerinde durulduğu görülmektedir. Daha önce de belirttiğimiz üzere doktrinde TCK m. 244'te yer alan suçların mala zarar verme suçunun özel bir şekli olduğu düşüncesi bulunduğu gibi, korunan hukuki değerin malvarlığı olduğu veya malvarlığının yanında sisteme olan güven, veriler, sistem vb. başkaca değerlerin de korunduğunu ifade eden görüşlerde mevcuttu. Bununla birlikte doktrinde TCK'nın sistematiğine bakıldığında suçların korunduğu hukuki değere göre tasnif edildiği ve hukuki değer esasına dayalı bir sıra izlendiği, bununla birlikte bilişim suçları düzenlenirken farklı hukuki değerleri koruyan hükümlerin bir araya konulduğu ve korunan hukuki değerin tespitinde karışıklık oluşturduğu yönünde görüşler bulunduğu ilk bölümde ifade edilmişti[875]. Bu kapsamda mala zarar verme suçu ile bilişim suçları arasında ilişki kurulurken, bilişim suçlarının "Topluma Karşı Suçlar" kısmında düzenlenmiş olması ile mala zarar verme suçunun "Kişilere Karşı Suçlar" kısmında düzenlenmiş olması hususu da ayrıca göze çarpmaktaydı. Bu durum göz önünde bulundurularak doktrinde burada korunan değerin malvarlığı olmadığı; sistem bütünlüğü ve güvenliği, toplum çıkarları, kişilerin bilişim sistemlerine olan güveni vb. değerlerin korunduğuna yönelik görüşler de bulunmaktaydı. Bununla birlikte daha önce de belirtildiği üzere TCK m. 244'ün madde gerekçesinde yer alan "*sistemlere yöneltilen ızrar fiillerini özel bir suç haline getirme…*"[876] ve sistemin "*fiziki varlığı ile işlemesini sağlayan tüm unsurlarını*"[877] kapsayacak şekilde topyekûn koruma altına alınması ifadeleri[878] de korunan hukuki değerin malvarlığı olduğunu savunan görüşü destekler nitelikte bulunmaktaydı. Mala zarar verme suçuyla TCK m. 244'te yer alan suçlar arasında kurulan ilişki ise sistemlere yönelik gerçekleştirilen zarar verici eylemlerin bu iki suç tipinden hangisi kapsamında değerlendirileceği hususunda önem arz etmektedir.

Klasik mala zarar verme suçunda söz konusu mal üzerinde fiziksel bir zararın gerçekleşmesi aranmaktayken, bilişim sistemlerinin yazılım unsurlarına yönelik

[875] Akbulut, *Bilişim Alanında Suçlar*, 102 vd.
[876] "Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu (1/593)", 156.
[877] "Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu (1/593)", 156.
[878] Dülger, *İnternet İletişim Hukuku*, 335.

müdahaleler her daim sistem üzerinde fiziksel etkiler göstermemektedir[879]. Bu sebeple bilişim sistemlerine ait veri ve programlar gibi soyut unsurların mala zarar verme suçu ile korunması sağlanamamakla birlikte, bilişim sisteminin somut unsurları olan donanım elemanlarının bu suçla koruma altına alınması mümkündür. Öğretide ise bilişim suçlarına yönelik düzenlemeler dâhilinde, bilişim sistemine yapılan fiziksel saldırıların sistemin içerisinde veri olup olmaması, failin saiki, eyleminin niteliği gibi farklı kriterlere göre suç tipi değerlendirilmiş ve buna göre mala zarar verme suçunu mu yoksa TCK m. 244'te yer alan suçu mu oluşturduğu belirlenmeye çalışılmıştır. Buna göre doktrinde bir görüşe göre, örneğin bilgisayarın doğrudan parçalanması gibi bir eylemde failin kastının yalnızca mala zarar vermek olması halinde mala zarar verme suçunun oluşacağı, ancak hedefin donanıma zarar vererek sistemin çalışmasını önlemek olduğu durumda TCK m. 244 kapsamında cezalandırılacağı ifade edilmektedir[880]. Başka bir görüşe göre ise bu tarz bir eylemin içinde veri bulunmayan bir sisteme karşı işlenmesi gibi bir durumda ya da verilere zarar vermeyen, veri işlemini engellemeyen nitelikte olması halinde mala zarar verme suçu kapsamında görülmesi gerekmektedir[881]. Aksi halde söz konusu eylemin TCK m. 244 kapsamında değerlendirilmesi gerekecektir. Bir diğer görüşe göre ise bilişim sistemi dışındaki unsurlara yapılan müdahaleler bozma ya da engelleme olarak kabul edilemeyecek olup taşınır bilgisayarın yere atılarak parçalanması gibi hallerde mala zarar verme suçu oluşacak, ancak; sisteme örneğin bir zararlı yazılım yüklenerek bilgisayarın çalışmasının engellenmesi durumunda ise TCK m. 244'te yer alan suç oluşacaktır[882]. Yine bu konuda başka bir görüşe göre ise; kanun koyucu bu tarz bir düzenlemeyi yazılım kısmını korumaya yönelik getirmiş olup donanım kısmı zaten TCK m. 151 kapsamında korunabildiğinden[883], yazılım unsuruna yönelik hareketler TCK m. 244/1 kapsamında, donanım unsuruna yönelik hareketler TCK m. 151 kapsamında değerlendirilmeli; fakat fiziki saldırılar hem yazılım hem donanımı etkilerse bu durumda her iki suç da

[879] Ketizmen, "Bilişim Suçları", 148.
[880] Dülger, *İnternet İletişim Hukuku*, 338.
[881] Akbulut, *Bilişim Alanında Suçlar,* 180.
[882] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1008.
[883] Ketizmen, *Türk Ceza*, 137.

oluşacağından, fail TCK m. 44 gereği en ağır suç olan TCK m. 244/1'den cezalandırılmalıdır[884].

Kanaatimce bilişim suçları ilk ortaya çıktığında her ne kadar mala zarar verme suçu ile koruma altına alınamayan soyut nitelikteki veri ve sistemlerin mülkiyet hakkının korunması amacıyla getirilmişse de, günümüzde bu sistemlerin korunmasında mülkiyet hakkı korunan tek hukuki değer değildir. TCK m. 244'ün gerekçesinde "ızrar" ifadesi kullanılarak mala zarar verme suçuyla korunamayan bu sistem ve verilere karşı mülkiyet yönüyle gerçekleştirilecek zarar verici eylemlere karşı korumanın sağlanması hedeflenmiştir. Bununla birlikte "işlemesini sağlayan" ifadesiyle bilişim sisteminin düzgün işleyişinin korunduğunu açık bir şekilde göstermiştir. Bu suçları topluma karşı suçlar kısmında düzenleyerek ise toplum çıkarları, kişilerin bilişim sistemlerine olan güveni, kamu düzeni ve ekonomik düzen gibi değerlerin korunmasının hedeflendiğini göstermiştir. Dolayısıyla bu suçla korunan hukuki değer karma bir nitelik göstermektedir. Bu kapsamda mala zarar verme suçunun özel bir şekli olmadığı da açık olarak gözükmektedir.

Daha önce de belirttiğim üzere; TCK m. 244'te yer alan düzenlemenin soyut ya da somut herhangi bir eylem şekli ifade etmediği görülmektedir. Eylemin fiziksel saldırılar yoluyla da gerçekleştirilebilmesi mümkündür. Ancak salt mala zarar verme amacıyla somut bir bilişim sistemine yönelik gerçekleştirilecek eylemler mala zarar verme suçu kapsamında değerlendirilmelidir. Çünkü TCK m. 244'te amaç bir bilişim sisteminin herhangi bir mal olarak değil bir bilişim sistemi olarak korunması hedeflenmektedir. Yani failin kastı bu sisteme bir bilişim sistemi olarak yönelmiş olmalıdır. Bununla birlikte fiziksel saldırılarla gerçekleştirilen eylem sonucu soyut nitelikteki unsurlara yönelik bir zarar meydana gelmişse bu durumda TCK m. 244/1-2 açısından failin olası kastının değerlendirilmesi gerekir. Böyle bir durumda fail tek eylemle her iki suç tipini de gerçekleştirmiş olacağından fikri içtima yapılması gerekmektedir. Ancak yine kanaatimce, kanunkoyucunun TCK m. 244'ü sistemin soyut unsurlarına mahsus bir düzenleme olarak getirmesi ve somut unsurlarına yönelik eylemler açısından bir nitelikli hal olarak mala zarar verme suçu kapsamında yer vermesi çok daha yerinde olurdu. Bununla birlikte; seri üretim halinde bulunan, içerisinde kullanıcı verisi yer

[884] Öndin, "Türk Hukukunda", 57.

almayan veyahut tahsis amacına özgü bir göreve atfedilmeyen, diğer bir ifadeyle, henüz kullanım aşamasında bulunmayan somut donanımsal nitelikte bir bilişim sistemine zarar verilmesi halinde TCK m. 244 kapsamında değerlendirilmemesi gerekir. Yine; amacına hizmet edecek şekilde çalışabilir durumda olmayan diğer bir ifadeyle iş göremez halde bulunan somut bilişim sistemleri için de aynı durum geçerlidir. Böyle bir halde eylemin doğrudan mala zarar verme kapsamında değerlendirilmesi gerekir. Çünkü böyle bir durumdaki bilişim sisteminin soyut unsurları herhangi bir kimse açısından TCK m. 244 anlamında bir değer ifade eder hale gelmemiştir.

2.6.2. Belgede Sahtecilik Suçlarıyla Karşılaştırılması

Bilişim alanındaki gelişmelerle birlikte fiziki olarak düzenlenen belge ve evrakların elektronik ortamda tutulabilmesi mümkün hale gelmiş, depolama, taşıma ve erişim kolaylığı gibi birçok faydası da göz önünde bulundurulduğunda evrak ve belgelerin sistemler üzerinden düzenlenmesi ve saklanması hem bireysel hem de kurumsal olarak tercih edilen bir yöntem olarak karşımıza çıkmıştır. Bu durum hukuki işlemlerin de elektronik ortama taşınması konusunu gündeme getirmiş ve 5070 Sayılı Elektronik İmza Kanunu gibi birtakım düzenlemeler kanun koyucu tarafından yürürlüğe konulmuştur. Bununla birlikte, elektronik ortamda düzenlenen belgelerin ceza hukuku bakımından nasıl değerlendirileceği problemi ortaya çıkmış, bilişim sistemleri üzerinden düzenlenen veri niteliğindeki belgelerin belgede sahtecilik suçları kapsamında değerlendirilip değerlendirilemeyeceği hususu ayrı bir tartışma konusu olmuştur.

Verilerin belgede sahtecilik suçunun konusunu oluşturup oluşturmayacağının belirlenebilmesi için öncelikle belgede sahtecilik suçunun konusunu oluşturan belgenin unsurlarının incelenmesi gerekmektedir. Bu suçlar kapsamında belgeden söz edilebilmesi için ilk olarak yazılı irade beyanı içeren bir nesne, ikinci olarak yazılı irade beyanın belirli bir kimseye izafe edilmesi, üçüncü olarak ise bu beyanın hukuki bir kıymete sahip olması gerekmektedir[885]. Bu unsurlar bağlamında incelendiğinde bir bilişim verisi cismani bir varlığı bulunmadığından ilk unsuru; imzanın güvenli

[885] Başar Pancaroğlu, "Bilişim Sistemlerindeki Veriler Bağlamında Belgede Sahtecilik Suçu", (Yüksek Lisans Tezi, Hacı Bayram Veli Üniversitesi, 2019): 201.; Özgenç, *Genel Hükümler*, 137-138.

elektronik imza ile imzalanmamış olması halinde ise ikinci unsur karşılayamamaktadır[886]. Belgenin güvenli elektronik imzayla imzalanması halinde ise her ne kadar 5070 Sayılı Kanun m. 5'te "Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur." hükmü düzenlenmiş olsa da doktrinde bu hükümle e-imzalı verinin hukuken hüküm ve sonuç doğurduğunu değil, yalnızca beyan iradesi unsurunu taşıdığını ifade ettiği belirtilmektedir[887].

Öğretide elektronik ortamdaki verilerin belgede sahtecilik suçunun konusunu oluşturmayacağı görüşü[888] baskındır. Diğer bazı görüşlere[889] göre ise güvenli e-imzalı veriler bu anlamda belge niteliğindedir. Bu görüşlerden birinde göre; güvenli elektronik imzayla imzalanmış verilerin belgenin bütün unsurlarını taşıdığını, bilişim sistemlerinin kanun koyucu tarafından kayıt ortamı olarak kabul edilmesi göz önünde bulundurulduğunda, güvenli e-imza ile imzalanmış verilerin belgede sahtecilik suçlarının konusunu oluşturacağı ifade edilmiştir[890]. Bununla birlikte e-imzalı belgenin çıktısının tek başına hiçbir hukuki sonuç doğurmayacağı ifade edilmektedir[891]. Başka bir görüşe göre ise sahtecilik suçları ile korunan hukuki değer bağlamında belgenin sanal ortamda bulunması ile fiziken bulunması arasında günümüz koşullarında önemli bir fark bulunmadığından güvenli e-imzalı belgeler sahtecilik suçuna konu olacaktır[892].

Sonuç olarak, ayrıyeten düzenlenmediği sürece elektronik ortamdaki verilerin ceza hukukunda belge sayılamamasından dolayı, ortada fiziki bir belge mevcut olmadığı için, söz konusu verilerin değiştirilmesi ya da sisteme yüklenmesi, öğretideki baskın görüşe göre TCK m. 204 veya 207'de yer alan suçları değil TCK m. 244/2'de yer alan suçu oluşturmakta bu da yaptırım açısından doktrinde bir ödüllendirme olarak nitelendirilerek AKSSS'de yer alan yükümlülükleri karşılamak noktasında yetersiz

[886] Pancaroğlu, "Belgede Sahtecilik",202.
[887] Pancaroğlu, "Belgede Sahtecilik", 202.
[888] Koca ve Üzülmez, *Özel Hükümler*, 862.; Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 947.; Pancaroğlu, "Belgede Sahtecilik", 203.; Çağda Nur Turhan, "Resmi Belgede Sahtecilik Suçu", (Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi, 2016), 16.; Özgenç, *Genel Hükümler*, 138.
[889] Arif Gözel, "Belgede Sahtecilik Suçlarının Konusu Olarak Belge ve Elektronik Belge", *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi,* 5/1 (2015): 159,188.; Niyazi Çiçek, "Hukuksal Geçerlilik Bakımından Resmi Belgelerin Biçimsel Özellikleri", *Amme İdare Dergisi*, 40/4 (2007), 137.;
Nurullah Tekin, "Resmi Belgede Sahtecilik Suçunda Bazı Özel Durumlar", *Türkiye Adalet Akademisi Dergisi*, 5/19 (2014), 935.
[890] Arif Gözel, "Elektronik Belge", 159,188.
[891] Tekin, "Belgede Sahtecilik", 936.
[892] Erkan, "Bilişim Sistemine", 144.

görülmektedir[893]. Bu konuda, AKSSS m. 7'de düzenlenen bilgisayarla bağlantılı sahtecilik eylemlerine yönelik suçların ceza hukukumuzda bir karşılığının bulunmadığı ve mevzuata buna yönelik düzenleme getirilmesinin gerekli olduğu ifade edilmektedir[894]. Bu durumu kanıtlar nitelikteki örnek bir kararda Yargıtay; "…*Somut olayda; şirketin yetkili temsilcisi olan sanığın katılan kurum ile yapılan sözleşmeye istinaden kurumun verdiği şifreyle sisteme hukuka uygun şekilde girerek, e-bildirge içeriğine doğru olmayan verileri yerleştirmesi sonucu kuruma elektronik ortamda gerçek olmayan bir beyanı iletmekten ibaret eyleminde atılı suçun açıklandığı üzere unsurları itibariyle oluşmadığı anlaşılmıştır…"* gerekçesiyle sanığın eylemi suç olarak kanunda tanımlanmadığından yerel mahkemenin özel belgede sahtecilik suçundan vermiş olduğu mahkûmiyet hükmünü bozarak sanığın beraatine karar verilmesi gerektiğine hükmetmiştir[895].

Yargıtay'ın verilerin belgede sahtecilik suçlarına konu olup olmayacağına ilişkin farklı kararları bulunmaktadır. Yargıtay 11. Ceza Dairesi 2019 yılında vermiş olduğu bir kararında fiziki olarak verilen belgenin varlığı halinde TCK m. 207'de yer alan özel belgede sahtecilik suçunun oluşacağını, elektronik ortamda verilmiş belgenin varlığı halinde TCK m. 206/1'de yer alan resmi belgenin düzenlenmesinde yalan beyanda bulunma suçunun oluşacağını kabul etmiştir[896]. Yargıtay Ceza Genel Kurulu ise 2017 tarihli bir kararında, elektronik ortamda bulunan ve e-imza ile imzalanmayan bir belgenin resmi belge niteliğinin bulunmayacağını, ancak e-imza ile imzalanması halinde resmi belge niteliğine kavuşacağını, dolayısıyla söz konusu belgenin e-imzalı belge olması halinde resmi belgede sahtecilik suçuna konu olacağını kabul etmiştir[897]. Ancak cismani varlığı bulunmayan verilerin e-imzayla imzalanmasının veriye belge vasfı katmayacağı gerekçesiyle bu karar doktrinde hukuka aykırı görülerek eleştirilmektedir[898]. Buna göre, e-imzalı verilerin belgede sahtecilik suçlarına konu

[893] Özsoy, "Doğrudan Bilişim Suçları", 334.
[894] Gün, "Bilişim Suçları", 243.
[895] Yılmaz, *Siber Suçlar,* 226. Yargıtay 11. Ceza Dairesi, 18.03.2021, E. 2018/6275, K. 2021/2806, https://karararama.yargitay.gov.tr/ E.T. 15.01.2025.
[896] Yargıtay 11. Ceza Dairesi, 28.02.2019, E. 2018/4004, K. 2019/2115, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.
[897] Yargıtay Ceza Genel Kurulu, 24.01.2017, E. 2016/1065, K. 2017/27, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.
[898] Pancaroğlu, "Belgede Sahtecilik", 212.

edilmesi halinde kıyas yasağının ihlali söz konusu olacaktır[899]. Yine Yargıtay Ceza Genel Kurulu'nun 2020 tarihli bir kararında ise; elektronik belgede sahtecilik eylemlerinde özel normun önceliği ilkesi gereği, belgede sahtecilik suçunun değil, TCK m. 244/2'nin uygulanması gerektiği ifade edilmiştir[900]. Yargıtay 5 Ceza Dairesi ise bir kararında; menfaat karşılığında sanığın iki soruşturma dosyasını savcı odalarından gizlice alıp ilgili savcıların şifrelerini kullanmak suretiyle giriş yaptığı UYAP ortamında soruşturma dosyalarında suç ve taraf silme, taraf ekleme işlemlerini gerçekleştirdiği olay hakkında gerçek içtima kuralları uyarınca TCK m. 205/1-son ve TCK m. 244/2 hükümlerinin uygulanmasına hükmetmiştir[901].

Görüldüğü üzere verilerin ceza hukuku bağlamında belgede sahtecilik suçuna konu olup olamayacağı tartışmalıdır. Tartışmanın temel nedeni verilerin belgede sahtecilik suçlarının konusunu teşkil eden belge kavramını karşılayamıyor olmasıdır. Her ne kadar yargı kararlarında ve doktrinde yer alan bazı görüşlerde e-imzalı dijital belgelerin belgede sahtecilik suçunu oluşturacağı kabul edilmişse de, bu yaklaşım hatalı olup kanunilik ilkesini ihlal etmektedir. Bu durumda eylem TCK m. 244 kapsamında değerlendirilmelidir. Bununla birlikte; dijital belgeler üzerinde gerçekleştirilecek sahtecilik eylemlerine yönelik mevcut bir düzenleme bulunmaması, kullanım yaygınlığı da göz önünde bulundurulduğunda büyük bir eksikliktir. Bu durum ceza kanununda dijital belgede sahtecilik suçlarının açık bir biçimde düzenlenmesini gerektirmektedir.

2.6.3. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar ile Karşılaştırılması

TCK'nın dokuzuncu bölümünde "Özel Hayata ve Hayatın Gizli Alanına İlişkin Suçlar" başlığı altında TCK m. 132 ila 140. Maddeleri arasında, Haberleşmenin Gizliliğini İhlal, Kişiler Arasındaki Konuşmaların Dinlenilmesi ve Kayda Alınması, Özel Hayatın Gizliliğini İhlal, Kişisel Verilerin Kaydedilmesi, Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme, Verileri Yok Etmeme Suçları düzenlenmiştir.

---

899 "*„Elektronik ortamda oluşturulmuş resmi veya özel belgelerle ilgili olarak, TCK'nın belgede sahtecilik suçlarına ilişkin hükümlerinin uygulanabilirliğini sağlamak için bir kanuni düzenleme yapılmasına ihtiyaç bulunmaktadır…"*; Özgenç, *Genel Hükümler*, 138.

900 Yargıtay Ceza Genel Kurulu, 29.09.2020, E. 2017/1122, K. 2020/381, https://karararama.yargitay.gov.tr/. E.T. 15.01.2025. ; Dülger, *İnternet İletişim Hukuku*, 362.

901 Gün, "Bilişim Suçları", 243.; Yargıtay 5. Ceza Dairesi, 03.07.2014, E. 2014/ 6872, K. 2014/7366, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.

Özel hayata ilişkin suçların işlenmesi günümüzün teknolojik gelişmeleriyle birlikte çoğu zaman bilişim sistemlerinin kullanılması yoluyla gerçekleştirilmekte ve bu suçların yanında bilişim suçlarının da işlendiği görülmektedir. Bu durum çoğu zaman tek fiille birden fazla suçun ihlali ile gerçekleşmektedir. Örneğin TCK m. 244/2 kapsamında var olan verilerin bir yerden başka bir yere gönderilmesi eyleminde söz konusu verilerin kişisel veriler olması durumunda fail hem TCK m. 244/2'yi hem de TCK m. 136'yı ihlal etmiş olacaktır. Bu durumda tek fiille birden fazla suç işlenmiş olacağından fikri içtima kurallarına göre[902] failin ağır olan suçtan cezalandırılması söz konusu olacaktır.

Yargıtay 8. Ceza Dairesi vermiş olduğu bir kararda[903], kart bilgilerini kopyalamak amacıyla ATM' ye sistem kurma eyleminin TCK m. 244/2-3 kapsamında değil TCK m. 136 kapsamında görmüş, Yargıtay 12. Ceza Dairesi ise bir kararında[904] mağdurun cep telefonunu kendi bilgisayarına bağlayarak içerisinde bulunan rehber ve media dosyalarının tamamını ele geçirip cep telefonundaki kayıtları silme eylemlerinin TCK m. 244/2, TCK m. 134/1 ve TCK m. 136/1 suçlarını oluşturduğuna hükmetmiştir[905].

2.6.4. Hırsızlık ve Dolandırıcılık Suçları ile Karşılaştırılması

Hırsızlık suçu TCK m. 142'de düzenlenmiş olup, madde metninde, zilyedinin rızası olmaksızın başkasına ait "taşınır bir malın" kendine ya da başkasına yarar sağlamak amacıyla alınması olarak düzenlenmiştir. Doktrinde bir görüş söz konusu malın ekonomik bir değere sahip olmasını ararken, diğer bir görüşe göre malın herhangi bir değere sahip olması yeterli olup, özellikle ekonomik bir değere sahip olması şart değildir[906].

Hırsızlık suçunun yer aldığı düzenlemenin bilişim sistemleri ve bilişim verileri açısından dikkat çeken noktası, söz konusu suçun konusunun taşınır bir mal olmasıdır. Daha öncede belirttiğimiz üzere, bilişim verileri ve sistem verileri hukuken mal vasfında

[902] Akbulut, *Bilişim Alanında Suçlar,* 212.
[903] Yargıtay 8. Ceza Dairesi, 07.07.2014, E: 2014/23, K: 2014/17639, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.
[904] Yargıtay 12. Ceza Dairesi 18.10.2017, E: 2016/10576, K: 2017/7642, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.
[905] Gün, "Bilişim Suçları", 242.
[906] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 623.

görülmemektedir. Bu sebeple düzenlemeye göre verilerin bu suçun konusunu oluşturamaması gerekir. Doktrinde de ifade edildiği üzere, verilerin bulunduğu sistem her ne kadar fiziki bir varlığa ve değere sahip olduğundan hırsızlık suçunun konusuna girebilecekse de; doğrudan fiziki varlığa sahip olmayan veriler mal niteliğinde sayılmadığından hırsızlık suçuna konu olamazlar[907]. Buna göre; örneğin, maddi değere sahip online oyun karakterleri veyahut kripto paralar her ne kadar bir değere sahip olsalar da hukuken mal niteliğine haiz olmadığından hırsızlık suçunun konusunu oluşturamayacaktır[908]. Bununla birlikte doktrinde teknolojinin gelişmesiyle parasal değerlerin sanal ortamda elektronik para, kripto para yahut sanal para gibi adlandırmalarla kullanılmaya başlanmasıyla, bu ekonomik değere sahip verilerin de hırsızlık suçuna konu edilmesi gerektiğine yönelik düşünceler de mevcuttur[909]. Bu görüşe göre para nesne olarak maliyet ve değere sahip olsa da, tarihsel süreçte çeşitli şekillere bürünen paranın esas değeri temsil ettiği alım gücü olup, günümüz teknolojik gelişmeleriyle birlikte veri formuna dönüşmüş olması, paranın tarihsel süreçteki değişiminin göz ardı edilmesi anlamına gelmektedir[910]. Veri formuna dönüşmüş haliyle para, borçlar hukuku ve ticaret hukuku açısından borç verilmesi, mal alımı gibi işlemlerde geçerli sayılabiliyorsa, ceza hukuku anlamında da suça konu edilebilmesi gerekmektedir[911]. Bu konuda açıkça verilerin nitelendirilmesinde hukuki bir eksiklik bulunduğu ve buna ilişkin bir düzenleme getirilmesi gerektiği ifade edilmektedir[912]. Yargıtay 13. Ceza Dairesi'nin 2017 tarihli bir kararında ise oyun karakterinin çalınmasını TCK m. 244/4 kapsamında değerlendirmiş, ekonomik değer taşısa dahi verinin taşınır bir mal haline gelmeyeceğini ifade etmiştir[913]. Bu sebeple hırsızlık suçunun konusu mal olduğundan, verinin zilyedinin rızası dışında alınması hırsızlık suçu kapsamında görülmemiş, TCK m. 244/4'ün konusunun veri olduğu belirtilerek TCK m. 244'teki suçun oluştuğu kanısına varılmıştır. Doktrinde bir görüş Roma

[907] Erkan, "Bilişim Sistemine"; 134.;Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 642.
[908] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 642.
[909] Erkan, "Bilişim Sistemine", 143.; Dülger, *İnternet İletişim Hukuku*, 518.
[910] Dülger, *İnternet İletişim Hukuku*, 518.
[911] Dülger, *İnternet İletişim Hukuku*, 518.
[912] Erkan, "Bilişim Sistemine", 154.
[913] Yargıtay 13. Ceza Dairesi, 10.10.2017, E. 2016/2155, K. 2017/10403, https://karararama.yargitay.gov.tr/, E.T. 15.01.2025.; Aköz, "Mevzuat Önerileri", 119.; Benzer şekilde; "…oyun karakterine ait sanal eşyanın maddi değerinin bulunduğu hususunun kuşkusuz olması ve sanığın bu karakteri kullanarak menfaat elde ettiğinin anlaşılması karşısında; sanığın eyleminin TCK.nın 244/4. maddesindeki suçu oluşturacağı gözetilmeden…": Yargıtay 8. Ceza Dairesi, 19.01.2022, E. 2019/23602, K. 2022/912, https://karararama.yargitay.gov.tr/ E. T. 15.01.2025.; Yılmaz, *Siber Suçlar,* 223.

Hukukundan miras kalan taşınır mal, mülkiyet, zilyetlik gibi kavramların günümüz ihtiyaçlarını karşılar nitelikte olmadığını, hırsızlık suçunu lafzi yorumla bağlı kalarak bu kavramlar yoluyla değerlendirmenin siber alanda gerçekleştirilecek fiillere kayıtsız kalmak anlamına geldiğini ve gai yorum yapılarak suçun tarifine ulaşma mecburiyeti ortaya çıkardığını; tüm bunlarla birlikte bilişim hırsızlığının ayrı bir suç olarak düzenlenmesi gerektiği ifade edilmektedir[914].

Doktrinde bir görüş, oyun karakterinin ekonomik değer karşılığının olmadığının ancak verinin ilk hali için söylenebileceğini, seviye atlanarak elde edilen tüm verilerin bir ekonomik değer getireceğini, bu sebeple hırsızlık suçu kapsamında görülmesi gerektiğini, yine NFT ve metaverse gibi uygulamalara yönelik ele geçirmelerin de aynı şekilde hırsızlık suçu kapsamında görülmesi gerektiğini, burada önemli olanın verinin alınıp satılırken ekonomik bir karşılığının bulunup bulunmadığı ve bu sebeple ekonomik değere karşılık gelen veri, sistem veyahut hesaplara yönelik eylemler açısından caydırıcı bir nitelikli hal düzenlenmesinin gerekli olduğunu ifade etmektedir[915]. Bununla birlikte yine aynı görüşe göre hesap ya da web sitesinin ele geçirilerek fidye istenmesi halinde eylem yağma suçu kapsamında görülmelidir[916].

Verilerin mal vasfında görülmemesi yalnızca belirtilen suç tiplerinde değil, diğer farklı suç tipleri açısından da etkili olmaktadır. Örneğin, Yargıtay bir kararında; TCK m. 155/2'de düzenlenen hizmet nedeniyle güveni kötüye kullanma suçunun oluşması için suçun konusunun eşya kapsamında değerlendirilebilmesinin gerektiğini, veriler eşya olarak değerlendirilemeyeceğinden somut olayda TCK m. 155/2'den değil, TCK m. 244'de yazılı suçtan hüküm kurulması gerektiğini ifade etmiştir[917].

TCK m. 142/1-e'de ise bilişim sistemlerinin suçun işlenişini kolaylaştırması göz önünde bulundurularak hırsızlık suçunun bilişim sistemleri aracılığıyla işlenmesi hali nitelikli hal olarak düzenlenmiş ve suçun basit haline göre daha ağır ceza öngörülmüştür. Ancak doktrinde bir görüşe göre bilişim sistemi aracılığıyla hırsızlık eyleminde suçun

[914] Murat Volkan Dülger ve Onur Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi", içinde *Prof. Dr. Mehmet Emin Artuk'a Armağan*, ed., Mahmut Koca, (Ankara: Seçkin Yayıncılık, 2020), 987.
[915] Demirci, *Soruşturma Yöntemleri*, 123.
[916] Demirci, *Soruşturma Yöntemleri*, 122.
[917] Yargıtay 11. Ceza Dairesi, 18.09.2013, E. 2012/2764 K. 2013/13257, Aktaran; Özsoy, "Doğrudan Bilişim Suçları", 344.

konusunun veri olacağı, bu sebeple de hırsızlık suçuna konu olamayacağı ifade edilirken[918]; bir diğer görüşe göre verinin hırsızlık suçuna konu edilip edilememesiyle taşınır bir malın bilişim sistemleri aracılığıyla çalınması ayrı hususlar olup bilişim sistemleri aracılığıyla hırsızlık suçunun işlenemeyeceği anlamına gelmemektedir[919]. Buna örnek olarak bilişim sistemlerinden faydalanılarak otomatik yükleme gerçekleştirilen bir yerde sistem kırılarak vincin çalıştırılıp ürünlerin kendi araçlarına yüklenmesi ve bu şekilde nitelikli hırsızlık suçunun gerçekleşmesi söz konusu olabilir[920].

Doktrinde bir görüş; hırsızlık suçunun bilişim sistemleri ile işlenmesi nitelikli hal düzenlemesinin bilişim sistemiyle kilitlenmiş bir kasa ya da kapının açılması gibi birkaç ihtimal dışında[921] uygulama imkanı olmadığını[922], uygulayıcıları ikileme sokar nitelikte bulunduğunu, veri mal vasfı taşımadığından ve kanunda ekonomik değer taşıyan enerji kavramı gibi ayrıca tanımlanmadığından bilişim sistemleri vasıtasıyla yapılan haksız kazanç kazanımlarının hırsızlık suçu kapsamında görülemeyeceğini ve tüm bu sebeplerle nitelikli hal olarak düzenlenmesinin mantıklı bir izahının olmadığını belirtmektedir[923]. Yargıtay'ın internet bankacılığı hizmetinden yararlanan mağdurun şifresini ele geçiren sanığın hesap bilgilerine eriştikten sonra banka hesabındaki parayı sahte bir kimliğe havale çıkarttığı olaya ilişkin vermiş olduğu kararında, suçun tamamlanma anını da bilişim sisteminin bu amaçla kullanıldığı zaman olarak değerlendirerek, TCK m. 142/2-e'de yer alan nitelikli hali uygulamıştır[924]. Yine sanığın internet sayfasına erişim sağlayarak birden fazla GSM hattına kontör yüklediği bir olayda 2022 tarihli bir kararda; "*sanığın amaç ve kastının var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği ve ekonomik bir değeri olan, ancak bir bedel ödemek suretiyle alınabilecek olan kontörleri alarak mal edinmeye yönelik*

[918] Bük, *Verilerin Korunması*, 125.; Yazıcıoğlu, *Bilgisayar Suçları*, 267.
[919] İsa Başbüyük, "Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi", *Ceza Hukuku Dergisi*, 5/4 (2010) : 164. www.jurix.com.tr/.
[920] Başbüyük, "Hırsızlık ve Dolandırıcılık", 163,
[921] Mahmutoğlu, "Yargı Kararları Işığında", 880.; Yazıcıoğlu, "Yeni Türk", 106.
[922] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1050.
[923] Mahmutoğlu, "Yargı Kararları Işığında", 880.; Yazıcıoğlu, "Yeni Türk", 104, 106.
[924] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1051.; Yargıtay 6. Ceza Dairesi, 02.06.2008, E. 2008/555, K. 2008/12249, https://kararara ma.yargitay.gov.tr/ E.T. 15.01.2025.

olduğunun anlaşılması…" gerekçesiyle TCK m. 244/4'ün değil; TCK m. 142/2-e'nin uygulanması gerektiğine hükmetmiştir[925].

Kanaatimce düzenleme mevcut haliyle incelendiğinde hırsızlık suçunun konusu taşınır mallar olduğundan, bu vasıfta olmayan dijital verilerin -her ne kadar maddi bir değere sahip olsalar da- hırsızlık suçunun konusunu oluşturamayacağı açıktır. Daha önce mala zarar verme suçuna ilişkin tartışmalarda da görüldüğü üzere dijital veriler nasıl mala zarar verme suçuna konu olamıyorlarsa aynı şekilde hırsızlık suçuna da konu edilemeyeceklerdir. Ancak kripto para, online oyun karakteri gibi dijital verilerin de maddi değere sahip olduğu bir gerçektir. Kanunilik ilkesi gereğince bu verilerin mevcut düzenleme yönüyle hırsızlık suçunun koruma kapsamı dışı kaldığı ve ancak kıyas niteliğinde bir değerlendirme ile hırsızlık suçuna konu edilebileceği ortadadır. Dolayısıyla burada TCK m. 142/2-e'nin değil, TCK m. 244/4'ün uygulanması gerekmektedir. Bununla birlikte; TCK m. 142/1-e'de yer alan düzenlemenin mevcudiyeti açısından bilişim sistemlerinin sağladığı kolaylıktan faydalanarak taşınır mallara yönelik hırsızlık suçunun işlenmesi yönüyle yerinde bir düzenleme olduğu ifade edilmelidir. Günümüzde bilişim teknolojilerinin suçta kullanılması giderek yaygınlaşmakta olup yalnızca bilişim sistemlerine yönelik gerçekleştirilen suç tiplerinde değil, kasten öldürme, yaralama ve hırsızlık gibi klasik suç tiplerinin işlenmesinde de oldukça etkili hale gelmiştir. Bu suretle gerçekleştirilen eylemler failin hedefine ulaşmasını oldukça kolaylaştırmakta ve çoğu zaman ortaya çıkan zararın ağırlığını artırmaktadır. Dolayısıyla klasik suçlar açısından eylemin bilişim teknolojileri kullanılmak suretiyle işlenmesi halinin bir nitelikli hal olarak düzenlenmesi son derece yerindedir.

TCK m. 157'de Dolandırıcılık Suçu, hileli davranışlarla bir kimseyi aldatarak, onun veya başkasının zararına olacak şekilde kendisine veya bir başkasına yarar sağlanması olarak düzenlenmiştir. Bu suçun TCK m. 158/1-f'de bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi ise nitelikli hal olarak görülmüştür. Bu nitelikli halde hileli davranışın gerçek iradeye yöneltilmesi ve gerçek iradenin fesada uğraması gerekmekte olup, gerçek kişiye yönelik hileli davranış

[925]Yargıtay 8. Ceza Dairesi, 15.03.2022, E. 2019/25433, K. 2022/4436, https://kararara ma.yargitay.gov.tr/ E.T. 15.01.2025.; Yılmaz, "*Siber Suçlar*", 223.

gerçekleştirilmeksizin veriler üzerinde değişiklik yapılarak haksız bir kazanç elde edilmesi durumunda dolandırıcılık suçu oluşmayacak[926]; bu durumda yerine göre TCK m. 244/4'te yer alan bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu veyahut TCK m. 142/2-e'de yer alan suç söz konusu olacaktır. Ancak gerçek kişiye karşı gerçekleştirilen hileli bir davranış söz konusuysa bu durumda TCK m. 158/1-f oluşmuş olacaktır. Örneğin; bedava hizmet sunduğunu belirten bir web sitesine girildiğinde siteye giren kişilere fatura yansıtılıyorsa bu nitelikli hal oluşacaktır[927]. Yine internet üzerinden rezervasyon yapılan ve ödeme sağlanan bir otelin bilişim sistemine girilerek rezervasyon yapan fail ödemeleri yapıldı gösterecek şekilde sisteme gerçeğe aykırı veri yerleştirirse, otele geldiğinde de otel yetkilisi sistemde ödemeyi görerek aldanıp failin kalmasına izin verirse bu nitelikli hal oluşacaktır[928]. Ancak doktrinde bir görüş yalnızca hileli davranışın bir insana yöneltilmesi gerekliliği üzerinden bu suçun değerlendirilmesinin yeterli olmadığını, bu konuda rızanın varlığının tespitinin gerektiğini, phishing yöntemiyle gerçekleştirilen eylemlerde, mağdurun malvarlığındaki eksilme mağdurun bu konudaki rızası elde edilmeden gerçekleştirildiğinden TCK m. 158/1-f kapsamında değerlendirilemeyeceğini, böyle bir durumda eylemin TCK m. 142/1-e kapsamında değerlendirilmesi gerektiğini ifade etmektedir[929]. TCK m. 158/1-f'deki nitelikli halin gerçekleşmesi noktasında önemli bir husus da suç kapsamında sistemin kullanımının rastgele olmaması hile ile eş zamanlı ve yoğun olması, hileli hareketin harici bir ortamda gerçekleşmesi değil, bir bilişim sistemi ortamında gerçekleşmesinin gerekli olmasıdır[930].

Doktrinde 158/1-f'deki düzenlemenin gereksiz olduğuna ilişkin düşünceler mevcuttur. Buna göre bir görüş, 158/1-f'de hilenin insana karşı yapılmış olmasının gerekliliği karşısında uygulama alanının bulunmadığını, TCK m. 244/4'ün varlığı karşısında gereksiz bir düzenleme olduğunu[931]; başka bir başka görüş ise, TCK m. 142/1-e ile TCK m. 158/1-f'de yer alan düzenlemelerin TCK m. 244/4'ün uygulama alanını daraltma

[926] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 748.
[927] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 805; Koca ve Üzülmez, *Özel Hükümler*, 818.
[928] Bük, *Verilerin Korunması*, 127. Kurt, *Açıklamalı - İçtihatlı,* 172.
[929] Fulya Korkmaz, "Dolandırıcılık Suçunun Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 69/3 (2020), 1428.
[930] Nurşen Selen Agin, "Türk Ceza Hukuku'nda Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu (TCK md. 158/1-f)" (Yüksek Lisans Tezi, İstanbul Üniversitesi, 2019), 104.
[931] Veli Özer Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 9/Özel Sayı (2007), 1059.

amacı güttüğü ifade etmektedir[932]. Ancak kanaatimce bilişim sistemlerinin TCK m. 244/1-2'deki eylemler gerçekleştirilmeden de dolandırıcılık suçunda araç olarak kullanılabileceği düşünüldüğünde TCK m. 158/1-f'nin gerekli bir düzenleme olduğu görülmektedir. Teknolojinin gelişmesiyle beraber internetin sunduğu geniş imkanlar dolandırıcılık suçu failleri için bilişim sistemlerini etkin bir araç haline getirmiştir. Günümüzde bilişim sistemleri üzerinden oldukça fazla sayıda dolandırıcılık eylemi gerçekleştirilmekte ve bu şekilde birçok insan mağdur edilmektedir. Bilişim sistemlerinin bu suçlarda araç olarak kullanılması faillerin işini kolaylaştırmakta, çok daha fazla kişiye kolay bir şekilde ulaşarak etki çevresini artırmasını sağlamakta ve yakalanma ihtimalini düşürerek cesaretlerini artırmaktadır. Dolayısıyla böyle bir düzenlemenin mevcudiyetinin gerekliliği TCK m. 244/4'ten bağımsız değerlendirilmelidir.

Günümüzde bankacılıkla ilgili birçok iş ve işlem internet bankacılığı üzerinden sanal ortamda yapılabilmekte ve insanlar tarafından da sıkça kullanılmaktadır. İnternet bankacılığı işlemleri bakımından ise örneğin bir kimseye ait hesabın şifrelerinin kırılması ya da bir bankanın sistemine girilerek başkasına ait hesaplardan para transferi yapılması gibi bir durumda TCK m. 244'ün mü yoksa TCK m. 158/1-f veya TCK m. 142/2-e'nin mi uygulama alanı bulacağı tartışması ortaya çıkmaktadır[933]. Bu konuda, TCK m. 142/2-e'de yer alan suçun uygulanıp uygulanamayacağına dair tartışma temelde suçun konusunun belirlenmesi noktasında ortaya çıkmaktadır. Yargıtay 11. Ceza Dairesi'nin bir kararına göre[934] belirtildiği gibi bir örnek olayda failin eyleminde amaç hesapta yer alan paranın ele geçirilmesi olduğundan tamamen malvarlığına yönelik olup, hırsızlık suçunun konusunu oluşturacak ve TCK m. 244/4 eylemin başka suç oluşturmaması halinde kullanılacak yardımcı bir norm olduğundan TCK m. 142/2-e'den cezalandırma söz konusu olacaktır. Diğer görüş ise suçun basit şeklinin unsurlarının nitelikli hal için de geçerli olduğunu, suçun basit halinin konusunun taşınabilir mal olduğunu, verinin taşınır mal vasfında olmadığını, verinin ekonomik değeri bulunan kavramları temsil etmesinin veriyi taşınır mal haline getirmediğini ifade etmekte ve dolayısıyla TCK m. 142/2-e'nin böyle bir somut duruma

[932] Koca ve Üzülmez, *Özel Hükümler*, 1034.
[933] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1015.
[934] Yargıtay 11. Ceza Dairesi, E. 16731, K. 12235, Aktaran; Dülger, *İnternet İletişim Hukuku*, 513.

uygulanamayacağını, bu halde TCK m. 244/4'ten hüküm kurulması gerektiğini ifade etmektedir[935]. Bu konuda başka bir görüşe göre ise, paranın bankaya yatırılması ile birlikte paranın maliki ve zilyedi artık banka olduğundan, parayı bankaya yatıran kişinin mülkiyet ve zilyetlik hakkı sona ermekte ve tipiklik anlamında hırsızlık suçuyla örtüşmemekte; havale işleminin nesnesi ise alacak hakkını temsil eden, maddi varlığı bulunmayan kaydi para olduğundan TCK m. 142/2-e'de yer alan suç oluşmamaktadır[936]. Ele geçirilen internet bankacılığı şifresiyle hesaplar arası havale işlemi gerçekleştirilmesi durumunda, müşteri gibi davranan failin kandırmaya yönelik eylemi sisteme karşı olup gerçek bir şahsa karşı olmadığından TCK m. 158/1-f gerçekleşmeyeceği gibi; TCK m. 244/4'ün uygulanabilmesi için öncelikle TCK m. 244/1-2'de yer alan eylemlerin gerçekleştirilmesi gerekmekte olup, böyle bir durum da söz konusu olmadığından TCK m. 244/4'te ihlal edilmiş olmayacaktır[937]. Böylece bu suçlardan hiçbirini ihlal etmeyen söz konusu eylem cezasız kalacağından, bilişim sistemlerinin otomatik iradelerine yönelik her tür hileli eylemle yarar elde edilmesine yönelik bir suç tipi düzenlemesi getirilmesi gerekmektedir[938]. Bu görüşe katılmayan başka bir görüşe göre ise; burada bilişim sistemi aracılığıyla havale edilen para "veri" olduğundan ve TCK m. 244'te yer alan suç hırsızlık ile dolandırıcılık suçlarına göre özel norm niteliği taşıdığından söz konusu eylem TCK m. 244/4 kapsamında, eğer haksız çıkar sağlanması söz konusu değilse de TCK m. 244/1-2 açısından değerlendirilmelidir[939].

İnternet bankacılığına yönelik eylemlerin TCK m. 244, TCK m. 158/1-f ve TCK m. 142/2-e hükümlerinin hangisi kapsamında değerlendirileceği noktasındaki ayrılıklar Yargıtay kararlarına da yansımış, farklı dairelerce verilen çelişkili kararların ortaya çıkmasına sebep olmuştur[940]. Son olarak Yargıtay Ceza Genel Kurulu bu konuya noktayı koymuş ve eylemin verinin temsil ettiği parayı almak suretiyle mal edinmeye yönelik olduğunu belirterek verinin hırsızlık suçunun konusunu oluşturacağını kabul

[935] Mehmet Emre YILDIZ, "İnternet Bankacılığı Hakkında Yargıtay'ın 17.11.2009 Tarih, 2009/11-193 Esas Sayılı Kararının İncelenmesi", *Ceza Hukuku Dergisi*, 5/14 (2010), 147.
[936] Başbüyük, "Hırsızlık ve Dolandırıcılık", 168.
[937] Başbüyük, "Hırsızlık ve Dolandırıcılık", 172.; Mahmutoğlu, "Yargı Kararları Işığında", 882.
[938] Başbüyük, "Hırsızlık ve Dolandırıcılık, 172.
[939] Özbek, Doğan ve Bacaksız*, Özel Hükümler*, 1018.
[940] Bkz. Yargıtay 6. Ceza Dairesi, 02.06.2008, E. 2008/555, K. 2008/12249, https://kararara ma.yargitay.gov.tr/, E.T. 15.01.2025; Yargıtay 11. Ceza Dairesi, 27.04.2009, E. 964, K. 4877, Aktaran; Dülger, *İnternet İletişim Hukuku,*513-515.

etmiştir[941]. Bununla birlikte 17.11.2009 tarihli söz konusu kararda; *"…bilişim sistemleri aracılığıyla haksız çıkar sağlanmış olması halinde, öncelikle Yasa'da düzenlenmiş olan bilişim sistemlerinin kullanılması suretiyle işlenebilen diğer suçların oluşup oluşmadığı değerlendirilmeli, şayet gerçekleştirilen eylem bu suçlardan hiçbirisinin tanımına uygun değilse, o zaman 244. maddenin 4. fıkrası hükmü uyarınca uygulama yapılmalıdır…"*[942] denilmek suretiyle TCK m. 158/1-f veya TCK m. 142/2-e'nin uygulanabilecek olması durumunda TCK m. 244/4'ün uygulanamayacağı ifade edilmiştir. 17.11.2009 tarihli karardan önce verilmiş olan Yargıtay kararlarına bakıldığında eylemde gerçek kişiye yönelik hile ve desise bulunmadığı durumlarda, TCK m. 158/1-f yerine TCK m. 244/4. madde hüküm kurulurken[943], söz konusu karardan sonra TCK m. 158/1-f'nin uygulanamadığı hallerde TCK m. 142/2-e maddesi uygulanmaktadır[944].

Özetle; Yargıtay Ceza Genel Kurulu'nun 17.11.2009 tarihli kararından sonra uygulamada internet bankacılığına yönelik eylemler TCK m. 158/1-f ve TCK m. 142/2-e kapsamında incelenmektedir. Eylem bu iki madde kapsamında değerlendirilemediği takdirde ise şartları mevcutsa TCK m. 244/4 kapsamında görülmektedir. Bununla birlikte söz konusu kararın yerinde olmadığı, verinin temsil ettiği paranın kararda belirtildiği gibi suçun konusu olarak görülmesiyle, aslında gerçekleşen veri transferinin göz ardı edildiği gerekçesiyle doktrinde eleştirildiği görülmektedir[945]. Kanaatimce de paranın bankaya yatırılmasıyla artık hesaptaki para nesnelliğini yitirmekte, maddi varlığı olmayan ve kişiye alacak hakkı veren yani maddi değere sahip olan bir veri haline gelmektedir. Hesaptaki para bu haliyle hırsızlık suçunun konusunu oluşturmayacağından TCK m. 142/2-e'nin uygulanmaması gerekmektedir. Failin internet bankacılığı şifresini ele geçirerek hesaplar arası havale yapması durumunda ilk olarak sisteme girme; ikinci olarak var olan verinin başka yere gönderilmesi eylemi gerçekleşeceğinden, eylem bu yolla haksız bir çıkar elde edilmesi şartını da taşıyacağından TCK m. 244/4'ün ihlali gerçekleşmiş olacaktır. Dolayısıyla böyle bir

[941] Yargıtay Ceza Genel Kurulu, 17.11.2009, E. 2009/11-193, K. 2009/268, www.kazanci.com.tr, E.T. 15.01.2025.
[942] Yargıtay Ceza Genel Kurulu, 17.11.2009, E. 2009/11-193, K. 2009/268.
[943] Yargıtay 11. Ceza Dairesi, 18.09.2007, E. 2007/6963, K. 2007/5533, www.kazanci.com.tr, E.T. 15.01.2025.
[944] Yargıtay 11. Ceza Dairesi, 10.12.2009, E. 2007/1260, K. 2009/16657, Aktaran; Dülger, *İnternet İletişim Hukuku*, 528.
[945] Özbek, Doğan ve Bacaksız, *Özel Hükümler*, 1018.

durumda failin TCK m. 243 ve TCK m. 244/4 kapsamında cezalandırılması gerekmektedir.

Yargıtay'ın bilişim alanının suçta kullanılması noktasında bu konuya benzer bir biçimde internet sitelerinde verilen ilanlar sonucu gerçekleşen dolandırıcılık olaylarına ilişkin olarak TCK m. 158/1-f'de düzenlenen nitelikli halin mi yoksa TCK m. 158/1-g'de düzenlenen basın ve yayın araçlarının sağladığı kolaylıktan faydalanmak suretiyle nitelikli dolandırıcılık halinin mi oluştuğu konusunda da içtihat farklılıkları görülmüş olup;[946] Yargıtay Ceza Genel Kurulu bu konuda her iki nitelikli halin de gerçekleşeceğine ve bunun sonucunda daha ağır cezayı gerektiren TCK m. 158/1-f'den ceza verilmesi gerektiğine hükmederek tartışmaya noktayı koymuştur[947].

Doktrinde teknolojinin günümüzde evrildiği nokta itibariyle genel olarak bilişim suçları ve TCK m. 244/4'te düzenlenen suçların diğer suçlara nazaran ikinci planda kalması, hırsızlık ve dolandırıcılık suçları temelinde incelenirken veri ve kripto para gibi kavramların tartışmalı olması gibi hususlar göz önünde bulundurulduğunda hukukumuzda bilgisayar dolandırıcılığının bağımsız bir suç olarak düzenlenmesinin gerekli olduğu yönünde düşünceler mevcuttur[948].

Bilişim suçlarına yönelik mevcut düzenlemelerin kanunkoyucu tarafından oldukça geniş kapsamlı düzenlendiği görülmektedir. Kanunkoyucu bilişim sistemlerine ve verilere yönelik gerçekleştirilecek her türlü eylemin "Bilişim Alanında Suçlar" kısmında yer alan suç tipleriyle karşılanmasını sağlamaya çalışarak belirsiz ve genel bir alan oluşturmuştur. Failler tarafından bilişim sistemleri ve verilere yönelik gerçekleştirilecek birçok eylem bu maddeler kapsamında karşılık bulmaktadır. Bununla birlikte aslında suç işlenmesini kolaylaştıran ve etki kapsamı geniş olan bilişim suçlarının cezalandırma açısından yetersiz kalmasına neden olmaktadır. Bunun temel nedeni ise hırsızlık, belgede sahtecilik gibi suçlarda bilişim verilerinin suçun konusunda yer alan tanımlara

[946] Bkz: Beyza Melek Eryiğit, "Dolandırıcılık Suçu ve Özel Olarak Bilişim Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması Suretiyle Nitelikli Dolandırıcılık Suçu, (Yüksek Lisans Tezi, İstanbul Üniversitesi, 2019), 79.
[947] Eryiğit, "Dolandırıcılık Suçu", 82.; Yargıtay Ceza Genel Kurulu, 17.01.2017, E. 2015/15-867, K. 2017/13, https://kazanci.com.tr/, E.T. 15.01.2025.
[948] Ali Tanju Sarıgül, "Bilişim Teknolojisinde Bir Suistimal Örneği: Bilişim Sistemlerinin Kullanılması Suretiyle Dolandırıcılık Suçları", İçinde *Bilişim ve Teknoloji Hukuku Yıllığı 2022*, ed., Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar, (Ankara: Adalet Yayınevi, 2022), 99.

uygun bulunmaması dolandırıcılık suçu açısından bilişim sistemlerine karşı gerçekleştirilen eylemlerin tipikliği karşılamamasıdır. Böyle bir durumda kanunilik ilkesi gereğince faillerin bu suçların kapsamına girmeyen eylemlerinin TCK m. 244 kapsamında değerlendirilmesi gerekmektedir. Ancak yargının bu konuda aksine kararlar verdiği görülmektedir. Somut örnekleri değerlendirildiği üzere suç tanımlarına uymayan verilere ve sisteme yönelik eylemlerin klasik suçlar kapsamında değerlendirilmesi bu haliyle kanunilik ilkesine aykırılık teşkil etmektedir. Ancak kanunun mevcut haliyle de suç tipleri ve yaptırımları değerlendirildiğinde bilişim suçları diğer suçlardan yaptırım yönüyle daha hafif kaldığından, klasik suçlara göre özellikleri yönüyle daha ağır cezalandırılması gerekirken daha hafif cezalandırılarak failler açısından bir ödüllendirme haline gelmektedir. Faillerin gerçekleştirdiği eylemler ve etkileri aslında klasik suç tiplerinin daha üst bir seviyeye geçerek evrimleşmiş halidir. Dolayısıyla klasik suç işleme yöntemlerine göre daha ağır cezalandırılmasını gerektirmektedir. Tüm bu hususlar birlikte değerlendirildiğinde öncelikle bilişim alanına ilişkin kavramların belli bir düzleme oturtularak belirgin hale getirilmesi, ardından dijital verilere yani bilişim verilerine yönelik mülkiyet hakkının açıkça düzenlenmesi gerekmektedir. Bunun peşi sıra ise klasik suç tipleri ile bağlantılı olarak veyahut ayrı bir şekilde dijital veri hırsızlığı, bilişim dolandırıcılığı ve dijital belgede sahtecilik gibi suçların düzenlenmesi ve yaptırıma bağlanması gerekmektedir. Aksi takdirde görüldüğü üzere mevcut kanunun yetersizliği yargıyı kıyasa yol açacak ölçüde yorum yapmak suretiyle bu alandaki açığı kapatmaya itecek; kanunun belirsizliği ise hem doktrinde kafa karışıklığına ve tartışmalara yol açacak hem de yargıda birbirinden farklı zıt kararların ortaya çıkmasına sebep olarak hukuk sisteminin güvenilirliğini sarsacaktır.

SONUÇ

Bilişim sistemlerinin ortaya çıkışı son yüz yılda gerçekleşmiş olup insanlık tarihi açısından her ne kadar yeni bir gelişme olarak nitelendirilse de önemi sanayi devrimi ile mukayese edilmektedir. Dünyada teknoloji ve bilgi çağı dönemini başlatan bilişim sistemleri insanların günlük hayatını kolaylaştırdığı gibi; kötüye kullanılmaya başlanmalarıyla ceza hukukunu da ilgilendirmeye başlamıştır. İnternetin ortaya çıkışı ise bu tarz eylemleri yaygınlaştırmış ve bu suçların işlenme oranında pik oluşmasına zemin hazırlamıştır. İlk örnekleri ABD'de görülen bilişim suçlarına yönelik ilk düzenlemeler de burada yapılmış, peşi sıra diğer ülkelerin de yasal mevzuatlarına yansımaya başlamıştır. Bu suçlarla mücadelenin diğer klasik suçlara nazaran taşıdığı farklılıkların ve kovuşturmasında yaşanan zorlukların bir sonucu olarak ise uluslararası alanda işbirliğinin gerekliliği ortaya çıkmış; bu alanda 2001 yılında yürürlüğe giren Avrupa Konseyi Siber Suç Sözleşmesi taraf devletlerce imzalanarak, bu suçlara karşı birçok devletin katılımıyla uluslararası ölçekte dayanışma sağlanmaya çalışılmıştır. Türk Hukuku'nda 1989 yılına kadar bilişim kavramına yer verilmemiş olup, 1991'de gerçekleştirilen ilk düzenleme Fransız Godfrain Kanunu örnek alınarak 765 sayılı eski TCK'ya bilişim suçlarına ilişkin yeni maddeler eklenmesi suretiyle olmuştur. 2004'te çıkarılan 5237 sayılı TCK'da ise bu suçlar AKSSS sistemine paralel olarak ayrıntılı bir biçimde düzenlenmiş ve bilişim suçunun tanımı yapılmayarak eylemler temel alınmak suretiyle yaptırıma bağlanmıştır. Doğrudan bilişim suçları kanunun "Topluma Karşı Suçlar " başlıklı üçüncü kısmının 10. Bölümü olan "Bilişim Alanında Suçlar" bölümünde 243 ile 245. maddeleri arasında düzenleme bulmuş, dolaylı bilişim suçlarına ise kanununun ilgili muhtelif yerlerinde diğer suçların içerisinde yer verilmiştir. TCK m. 244/1'de bilişim sisteminin işleyişini engellemek, bozmak AKSSS m. 5'e paralel şekilde; TCK m. 244/2'de bir bilişim sistemi içindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir

yere göndermek AKSSS m. 4'e paralel şekilde suç olarak düzenlenmiştir. AKSSS'de verilere müdahale ile sisteme müdahale arasında bir sıra gözetilmişken TCK m. 244'te gözetilmemiş, sözleşmede eylemlerin haksız gerçekleştirilmesi aranırken TCK m. 244'te böyle bir şart belirtilmemiştir. Sözleşmenin 4. maddesinde bu suçların oluşmasında ciddi zarar şartı aranabileceği ifade edilmiş olsa da TCK böyle bir kıstas getirmemiştir.

TCK m. 244'de düzenlenen bu suçlarla bilişim sisteminin işleyişi ve kullanıcının veriler üzerindeki tasarruf yetkisi, toplum güveni, kamu düzeni ve ekonomik düzen, mülkiyet hakkı gibi birçok hukuki değer korunmaktadır. Suçun konusu ilk fıkra için bilişim sistemleri; ikinci fıkra için ise sistemde yer alan verilerdir. Bir bilişim sistemi olarak görülemeyecek, sadece depolama amacına hizmet eden USB bellek gibi aygıtlarda yer alan verilerin TCK m. 244 kapsamında değerlendirilmemesi gerekmektedir. Bu durumda böyle bir eylem mala zarar verme kapsamında değerlendirilebilecek olsa da zarar gören verilerin taşıyabileceği önem dikkate alındığında, sistem haricindeki veriler yönünden bir düzenleme eksikliği bulunduğu ifade edilmelidir.

TCK m. 244'de fail ve mağdur yönünden herhangi bir özel nitelik belirtilmediğinden herkes bu suçun faili ya da mağduru olabilir. Veriler üzerinde tasarruf yetkisi sahibinin belirlenmesi mağdurun tespiti açısından önemlidir. Ancak yetki sahibi kişi ya da kişiler her somut olayda değişiklik gösterebileceğinden bu konuda kesin bir kıstas belirlemek mümkün değildir. Her olayın somut özelliklerine göre bu konuda ayrıca belirleme yapılması gerekmektedir.

Madde metninde bilişim sisteminin engellenmesine yönelik saldırılara ilişkin soyut ya da somut herhangi bir eylem şekli ifade edilmediğinden, eylemin fiziksel saldırılar yoluyla da gerçekleştirilebilmesi mümkündür. Ancak kanunkoyucunun TCK m. 244'ü sistemin soyut unsurlarına mahsus bir düzenleme olarak getirmesi ve somut unsurlarına yönelik eylemler açısından bir nitelikli hal olarak mala zarar verme suçu kapsamında yer vermesinin çok daha yerinde olacağı ifade edilmelidir. Engellemenin geçici ya da kalıcı olması ise önem arz etmeyecektir. Bu noktada önemli olan sistemi engellemeye yönelik eylemin sistemin işleyişinin bozmayacak düzeyde kalmasıdır. Zararlı yazılımlar yoluyla sistemin yavaşlatılması halinde de sistemi engelleme eylemi gerçekleşmiş olacaktır.

TCK m. 244/2'de düzenlenen eylemler seçimlik hareketlerdir. Sayılan hareketlerden herhangi birinin gerçekleştirilmesi suçun gerçekleşmesi açısından yeterlidir. Veriye ilişkin bütün izlerin depolama ünitesinden silinmesi ile yalnızca veriye erişimi sağlayan anahtar verilerin silinmesi arasında yok etme eyleminin gerçekleşmesi açısından bir fark yoktur. Verinin kopyasının bulunup bulunmamasının ya da silinen verinin kopya olmasının da bir önemi yoktur. Verinin geri dönüşüm kutusuna atılması halinde ise veri dönüşüm kutusunda kaldığı müddetçe veri yok edilmiş olmayacak, bu durumda var olan veriyi başka yere gönderme eylemi gerçekleşmiş olacaktır. Verilerin yok edilmesi halinde özel bir takım cihazlar veya yöntemlerle verilerin geri getirilebilecek olması durumunda dahi yok etme eylemi gerçekleşmiş olacaktır. Önemli olan kullanıcının veriye normal yollarla ulaşamayacak hale getirilmiş olmasıdır. Verilerin gönderilmesi halinde gönderilen veri asıl veri ise, aynı bilişim sisteminin içerisinde, örneğin başka bir dosyaya gönderiliyorsa, bu durumda eylem verinin başka yere gönderilmesi olarak değerlendirilmelidir. Ancak veri, bulunduğu bilişim sisteminden başka bir bilişim sistemine kesilmek suretiyle gönderiliyorsa bu durumda verinin yok edilmesi olarak değerlendirilmesi gerekir. Fail hukuka aykırı şekilde bilişim sistemine girdikten sonra TCK m. 244/2 kapsamında herhangi bir eylemde bulunmadan yalnızca görerek verinin içeriğini elde edebilir. Bu durumda sisteme girme bakımından cezalandırılması söz konusu olacaksa da verinin içeriğini ele geçirmesi yönünden verilerin kişisel veri niteliğindeki veriler olması hali ile TCK m. 328 kapsamına giren haller hariç olmak üzere herhangi bir yaptırımla karşılaşmayacaktır. Failin sisteme hukuka uygun girmiş olması halinde ise hiçbir yaptırımla karşılaşmayacaktır. Bununla birlikte bu durumun temelinde verilerin hukuk düzenindeki yerinin netleştirilememesi sorunu bulunmaktadır.

Maddede düzenlenen bozma, yok etme, değiştirme, erişilmez kılma eylemleri bilişim sistemindeki verilere karşı gerçekleştirilecek birer sabotaj eylemi niteliğindedir. Bununla birlikte sisteme veri yerleştirme ve var olan verileri başka yere gönderme eylemleri ise birer casusluk eylemi niteliğindedir. Dolayısıyla aynı fıkrada düzenlenmeleri yerinde olmamıştır. Bununla birlikte, kanunkoyucunun kavramları kullanırken belirgin bir tanım yapmaktan kaçınması, eylemlerin tespiti ve sınıflandırılması bakımından belirsizliğe yol açmaktadır.

Birinci fıkrada sistemin engellenmesi ve bozulması, ikinci fıkrada verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme eylemleri aslında bir netice ifade ettiğinden bu suçlar serbest hareketli ve neticeli suçlardır. Özellikle bir zararın ortaya çıkması ise aranmamakta olup, şart değildir. Söz konusu suçlar tehlike suçudur.

TCK m. 244/3'te eylemlerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi bir nitelikli hal olarak düzenlenmiştir. Fıkrada belirtilen kurum ve kuruluşlarla sınırlama yapılması doğru değildir. Günümüzde özel şirketlere karşı yapılacak herhangi bir siber saldırı oldukça yıkıcı etkilere yol açabilmektedir. Kaldı ki kritik alanlarda faaliyet gösteren şirketlere yapılacak saldırılar yalnızca o şirketi değil, bir ülkeyi hatta dünya genelini etkileyecek zararlara yol açabilmektedir. Özellikle büyük bilişim şirketlerine yapılacak saldırılar, bu şirketlerle verilen hizmetlere bağlantılı olarak iletişim, enerji ve ulaşım gibi kritik hizmetlerin aksamasına yol açabilmektedir. Dolayısıyla TCK m. 244/3'te düzenlenen nitelikli hal banka, kredi kurumu, kamu kurum ve kuruluşuna ait sistemler açısından yerinde bir düzenleme oluştursa da, kamu özel ayrımı yapılmaksızın bir bütün şeklinde hizmetin korunmasına yönelik olarak tekrar düzenlenmesi son derece yerinde olacaktır. Cezanın belirlenmesi noktasında ise yalnızca bu nitelikli halle sınırlı olmaksızın, TCK m. 244'ün, genel olarak yetersiz kaldığını ifade etmek gerekir.

Doktrinde yer alan TCK m. 244'de yer alan suçların TCK m. 244/3'te yer alan kurumlarda görevli kişilerce bu kurumların sistemlerine karşı gerçekleştirilmesi halinin nitelikli hal olarak düzenlenmesi gerektiğine yönelik görüş son derece yerindedir.

Bununla birlikte TCK m. 244/3'te yer alan nitelikli halin tüm hizmetin korunmasına yönelik olarak düzenlenmesi gerektiği düşüncesiyle bağlantılı olarak, kamu görevlileri bakımından getirilecek nitelikli halin kritik hizmet faaliyetini yürüten özel şirketlerde çalışan kişileri de kapsar nitelikte oluşturulması gerekmektedir.

TCK m. 244/4'te ise TCK m. 244/1-2'deki eylemlerle kişinin kendisi veya başkası yararına haksız çıkar sağlaması bir nitelikli hal olarak düzenlenmiştir. Doktrinde ağırlıklı görüş düzenlemenin ayrı bir suç olduğu yönündedir. Bununla birlikte temel suç

tipine bağlılığı devam ettirdiği görüldüğünden nitelikli hal olarak değerlendirilmesi gerektiği ifade edilmelidir.

TCK m. 244/1-2'de yer alan suç için hukuka uygunluk nedenleri ilgilisinin rızası, meşru savunma ve görevin ifası/ Kanun hükmünün icrası olarak görülmekte, başkaca bir hukuka uygunluk nedeni bulunmamaktadır. Suçun kasten işlenmesi yeterli görülmüştür. Taksire ilişkin bir düzenleme bulunmadığından bu suçlar taksirle işlenememektedir. Failin saiki ise birinci ile ikinci fıkranın ayrımı açısından önemli olduğundan üzerinde durulması gerekmektedir. TCK m. 244 kapsamında düzenlenen tüm suçlara teşebbüs mümkün olup dolayısıyla gönüllü vazgeçme de mümkündür. Bu suçlarda iştirak yönünden ise özel düzenleme bulunmayıp genel hükümler uygulanır.

İçtima hususu değerlendirilecek olursa; TCK m. 243 ile TCK m. 244'ün birlikte ihlali halinde TCK m. 244 açısından sisteme girme zaruri bir eylem olmadığından, somut olayın özelliklerine göre değerlendirilerek, tek fiille her iki suç tipinin ihlalinin söz konusu olması halinde fikri içtima yapılması gerektiği ifade edilmelidir. TCK m. 244/1 ve TCK m. 244/2'deki suçların her ikisinin birlikte gerçekleştirilmesi halinde doktrinde bir görüşe göre, tek fiille farklı suçlar gerçekleştiğinden fikri içtima uygulanarak sorunun çözümlenmesi gerektiği, ikinci görüşe göre ise TCK m. 244/2'deki hareketler TCK m. 244/1'e vücut verdiyse TCK m. 244/1'deki suç kapsamında faile ceza verilmesi gerektiği ifade edilmişse de burada failin saikine bakılması gerekmektedir. Failin tek fiille hem TCK m. 244/2 hem de TCK m. 151'i ihlal etmesi halinde maddenin asli düzenlenme amacı bilişim sisteminin düzgün işleyişi ve sistemdeki verilerin korunması olduğundan salt mala zarar verme amacıyla somut bir bilişim sistemine yönelik gerçekleştirilecek eylemler mala zarar verme suçu kapsamında değerlendirilmelidir. Eylem sonucu soyut nitelikteki unsurlara yönelik bir zarar da meydana gelmişse bu durumda TCK m. 244/1-2 açısından failin olası kastının değerlendirilmesi gerekir. Bununla birlikte; seri üretim halinde bulunan, içerisinde kullanıcı verisi yer almayan veyahut tahsis amacına özgü bir göreve atfedilmeyen, diğer bir ifadeyle, henüz kullanım aşamasında bulunmayan somut donanımsal nitelikte bir bilişim sistemine zarar verilmesi halinde TCK m. 244 kapsamında değerlendirilmemesi gerekir. Yine; amacına hizmet edecek şekilde çalışabilir durumda olmayan diğer bir ifadeyle iş göremez halde bulunan somut bilişim sistemleri için de aynı durum

geçerlidir. Böyle bir halde eylemin doğrudan mala zarar verme kapsamında değerlendirilmesi gerekir. Çünkü böyle bir durumdaki bilişim sisteminin soyut unsurları herhangi bir kimse açısından TCK m. 244 anlamında bir değer ifade eder hale gelmemiştir.

TCK m. 244/1-2'de yer alan her iki suç için de kanunda yalnızca hürriyeti bağlayıcı ceza öngörülmüş olup adli para cezasına yer verilmemiştir. Doktrinde hem hürriyeti bağlayıcı ceza hem de adli para cezası düzenlenmesi ve seçimlik bir ceza öngörülmesi daha yerinde olacağı, TCK m. 244/2 açısından verilerin mağdur açısından önemine göre faile verilecek cezayı arttıracak nitelikte bir düzenlemenin yapılmasının uygun olacağı ifade edilmiştir. Bununla birlikte hem suçların niteliği hem de takibine ilişkin sorunlar açısından, düzenlemenin suçu önlemede yeterli olmadığı ve suçların işlenme sıklığı ile sebep olduğu zararın ağırlığı dolayısıyla cezanın alt sınırının oldukça düşük kaldığı vurgulanmıştır. Bilişim suçlarının ortaya çıkardığı tehlikenin boyutu göz önünde bulundurulduğunda cezalar oldukça hafif kaldığından ceza hukukunun caydırıcılık fonksiyonunu sağlamaktan uzaktır. Özellikle işlenmesindeki kolaylık ve anonim bir biçimde hareket serbestisi sağlayan yapısı, bu suçlarla mücadelede büyük zorluklar çıkarırken, caydırıcılık etkisi göstermeyecek derecede düşük seviye yaptırımların uygulanması potansiyel failler üzerinde gerçekçi bir etki uyandırmamaktadır. Eylemin yöneldiği tehlikenin boyutuna göre katmanlı bir yaptırım şekli düzenlenmesinde fayda vardır. Bu da hem temel cezanın üst sınırlarının artırılması, hem de risk oluşturduğu tehlikenin boyutlarına göre farklı nitelikli haller düzenlenmek suretiyle sağlanmalıdır.

Verilerin ceza hukuku bağlamında belgede sahtecilik suçuna konu olup olamayacağı tartışmalıdır. Tartışmanın temel nedeni verilerin belgede sahtecilik suçlarının konusunu teşkil eden belge kavramını karşılayamıyor olmasıdır. Her ne kadar yargı kararlarında ve doktrinde yer alan bazı görüşlerde e-imzalı dijital belgelerin belgede sahtecilik suçunu oluşturacağı kabul edilmişse de, bu yaklaşım hatalı olup kanunilik ilkesini ihlal etmektedir. Bu durumda eylem TCK m. 244 kapsamında değerlendirilmelidir. Bununla birlikte; dijital belgeler üzerinde gerçekleştirilecek sahtecilik eylemlerine yönelik mevcut bir düzenleme bulunmaması, kullanım yaygınlığı da göz önünde bulundurulduğunda büyük bir eksikliktir. Bu durum ceza kanununda dijital belgede sahtecilik suçlarının açık bir biçimde düzenlenmesini gerektirmektedir.

Fiziki varlığa sahip olmayan veriler mal niteliğinde sayılmadığından ceza hukukunda hırsızlık suçuna konu edilememekle birlikte doktrinde veri formundaki paranın, borçlar hukuku ve ticaret hukuku açısından geçerli sayılabildiği düşünüldüğünde, ceza hukuku anlamında da suça konu edilebilmesi gerektiği ifade edilmektedir. Bu durum ayrıca verilerin hukuki nitelendirmesinde eksiklik olduğu ve bu konuda kanuni düzenlemeye ihtiyaç duyulduğunu göstermektedir. Düzenleme mevcut haliyle incelendiğinde hırsızlık suçunun konusu taşınır mal olduğundan, maddi değere sahip olsalar dahi taşınır mal vasfında olmayan dijital verilerin hırsızlık suçunun konusunu oluşturamayacağı açıktır. Dolayısıyla suçun konusunun veriler ya da sistemin soyut unsurları olması halinde TCK m. 142/2-e'nin değil, TCK 244/4'ün uygulanması gerekmektedir. TCK m. 142/1-e'de yer alan düzenlemenin mevcudiyeti açısından ise günümüzde bilişim teknolojilerinin suçta kullanılması giderek yaygınlaştığından klasik suç tiplerinin işlenmesinde de oldukça etkili hale gelmiştir. Dolayısıyla klasik suçlar açısından eylemin bilişim teknolojileri kullanılmak suretiyle işlenmesi halinin bir nitelikli hal olarak düzenlenmesi yerindedir. Failin internet bankacılığı şifresini ele geçirerek hesaplar arası havale yapması durumunda hesaptaki para maddi değere sahip olan ancak maddi varlığı olmayan bir veri halinde bulunduğundan hırsızlık suçuna konu olamaz. Bu halde TCK m. 142/2-e'nin uygulanmaması gerekmektedir. Dolayısıyla böyle bir durumda failin TCK m. 243 ve TCK m. 244/4 kapsamında cezalandırılması gerekmektedir.

TCK m. 158/1-f'de dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi düzenlenmiştir. Bu nitelikli hal hileli davranış gerçek iradeye yöneltilmesi ve gerçek iradenin fesada uğratılması halinde gerçekleşmektedir. Teknolojinin gelişmesiyle beraber dolandırıcılık suçu failleri için bilişim sistemleri etkin bir araç haline gelmiştir. Dolayısıyla TCK m. 158/1-f'nin gerekli bir düzenleme olduğu görülmektedir. Ancak gerçek kişiye yönelik hileli davranış gerçekleştirilmeksizin veriler üzerinde değişiklik yapılarak haksız bir kazanç elde edilmesi durumunda dolandırıcılık suçu oluşmamaktadır. Bununla birlikte hileli eylemin verilere yönelik TCK 244'te yer alan eylemlerde bulunulmaksızın bilişim sistemlerine karşı gerçekleştirilmesi halinde ise eylemin bütün bir biçimde yaptırımsız kalması sonucuna ulaşılmaktadır. Bu durum bilişim sistemlerine karşı gerçekleştirilen hileli eylemlere yönelik ayrı bir düzenleme getirilmesini gerektirmektedir.

Çalışmada değerlendirildiği üzere TCK m. 244'e dair birden fazla konuda doktrinde görüş ayrılıkları bulunduğu ve düzenlemede eksik hususlar tespit edildiği görülmektedir. Bu konuda farklı görüşlerini ortaya çıkmasının temel sebebi kanun koyucunun bu suçları düzenlerken açık bir nokta bırakmak istememesi ve tam bir koruma sağlanmasını amaçlaması nedeniyle genel bir düzenleme yapması ve ileride ortaya çıkacak teknolojik gelişmelere uyum sağlamak maksadıyla bazı muğlak ifadeler kullanmasıdır. Uygulamada ise yargı bazında birçok konu oturtulmuş ve belli bir görüş benimsenerek faillerin cezalandırılması yoluna gidilmişse de bu süreçte gerek çelişkili gerek kanunilik ilkesini zedeleyen kararlar verildiği görülmüştür.

Kanunkoyucu bilişim sistemlerine ve verilere yönelik gerçekleştirilecek her türlü eylemin "Bilişim Alanında Suçlar" kısmında yer alan suç tipleriyle karşılanmasını sağlamaya çalışarak genel bir alan oluşturmuştur. Özellikle hırsızlık, belgede sahtecilik gibi suçlarda bilişim verilerinin suçun konusunda yer alan tanımlara uymaması dolandırıcılık suçu açısından ise hileli eylemin bilişim sistemlerine karşı gerçekleştirilmesi hali açısından tipikliği karşılamaması eylemlerin bu suçlar kapsamında değerlendirilememesine neden olmaktadır. Failler tarafından bilişim sistemleri ve verilere yönelik gerçekleştirilecek birçok eylem bu maddeler kapsamında karşılık bulmaktadır. Faillerin gerçekleştirdiği eylemler ve etkileri aslında klasik suç tiplerinin daha üst bir seviyeye geçerek evrimleşmiş hali olduğu halde mevcut düzenleme eksikliğiyle suç işlenmesini kolay ve etkili hale getiren bilişim suçlarının cezalandırma açısından yetersiz kalmasına neden olmaktadır. Tüm bu hususlar birlikte değerlendirildiğinde öncelikle; bilişim alanına ilişkin kavramların belirgin hale getirilmesi ve dijital veri mülkiyeti, veri hırsızlığı, bilişim dolandırıcılığı ve dijital belgede sahtecilik konularında kanuna açık düzenleme getirilmesi gerekmektedir. Aksi takdirde mevcut kanunun yetersizliği yargıyı kıyasa yol açacak ölçüde yorum yapmak suretiyle bu alandaki açığı kapatmaya itecek; kanunun belirsizliği ise hem doktrinde kafa karışıklığına ve tartışmalara yol açmaya devam edecek hem de yargıda birbirinden farklı zıt kararların ortaya çıkmasına sebep olarak hukuk sisteminin güvenilirliğini sarsacaktır.

KAYNAKÇA

Agin, Nurşen Selen. "Türk Ceza Hukuku'nda Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu (TCK md. 158/1-f)". Yüksek Lisans Tezi, İstanbul Üniversitesi, 2019)

Aliusta, Cahit ve Recep Benzer. "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci". *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4/2 (2018): 35-42.

Akarslan, Hüseyin. *Bilişim Suçları*. Ankara: Seçkin Yayınları, 2015.

Akarslan, Hüseyin. "Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı". Yüksek Lisans Tezi, T.C. Polis Akademisi, 2011.

Akbulut, Berrin. *Bilişim Alanında Suçlar*. Ankara: Adalet Yayınevi, 2017.

Akbulut, Berrin Bozdoğan. "Bilişim Suçları". *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*. 8/1-2 (2000): 545-555.

Akbulut, Berrin. "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme". *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*. 24/2 (2016): 7-55.

Akça, Kürşat. "Anayasa Mahkemesi Kararlarında Mülkiyet Hakkı". *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 6/3 (2016): 543-596.

Akıncı, Hatice, A. Emre Alıç ve Cüneyd Er. "Türk Ceza Kanunu ve Bilişim Suçları". İçinde *İnternet ve Hukuk*, editör Yeşim M. Atamer, 157-276. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004.

Aköz, Burak Cesur. "Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları İle Örnek Yargısal Kararların Analizi Ve Mevzuat Önerileri". Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2018.

Aksakallı, Işıl Karabey. "Bulut Bilişimde Güvenlik Zafiyetleri, Tehditler Ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi.". *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*. 5/1 (2019): 8-34. https://www.researchgate.net/publication/334155099_BULUT_BILISIMDE_GUVENLIK_ZAFIYETLERI_TEHDITLER_VE_BU_TEHDITLERE_YONELIK_GUVENLIK_ONERILERININ_INCELENMESI

Altunok, Ebru. "Bilişim Suçları". *Denetişim Dergisi*. 8 (2011): 74-84.

Apaydın, Cengiz. *Bilişim Sistemine Girme, Engelleme ve Bozma Suçları*. Ankara: Seçkin Yayınları, 2023.

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

Artuk, Mehmet Emin, Ahmet Gökçen ve Ahmet Caner Yenidünya. T*ürk Ceza Kanunu Şerhi Özel Hükümler Madde 235-345, 5. Cilt*. Ankara: Turhan Kitabevi, 2009.

Artuk, Mehmet Emin, Ahmet Gökçen ve Ahmet Caner Yenidünya. *Ceza Hukuku Özel Hükümler*. Ankara: Adalet Yayınevi, 2015.

Avcı, Mustafa. "TCK, Tasarılar ve 2004 TCK Tasarısı'nın Genel Olarak Değerlendirilmesi". İçinde *Türk Ceza Kanunu Reformu İkinci Kitap Makaleler, Görüşler, Raporlar*, editör Teoman Ergül, 199-232. Ankara: Türkiye Barolar Birliği Yayınları, 2004.

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

Avşar, B. Zakir ve Gürsel Öngören. *İnternet Hukuku*. Ankara: TOBB Yayınları, 2009.

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

Aysel Aksu. "Ağ Protokolleri". Erişim Tarihi 15.01.2025, https://sudo.ubuntu-tr.net/ag-protokolleri

Aytekin, Akın, Mehmet Serkan Kılıç ve Hüseyin Çakır. "Karşılaştırmalı Hukuk Açısından Siber Suçlar". içinde *Güncel Tehdit: Siber Suçlar*. editör Hüseyin Çakır ve Mehmet Serkan Kılıç. 180-204. Ankara: Seçkin Yayınları, 2014.

Balcı, Murat. "Yapay Zeka ve Ayrımcılık". İçinde *Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı*, ed. Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar, 329-350. Ankara: Adalet Yayınevi, 2021.

Baş, Eylem. *Ceza Hukukunda Fail ve Mağdur.* Ankara: Seçkin Yayıncılık, 2021.

Başbüyük, İsa. "Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi". *Ceza Hukuku Dergisi*. 5/4 (2010): 151-192. https://www.jurix.com.tr/article/2976?u=0&c=0.

Başlar, Yusuf. "Elektronik Delilin Toplanması ve Muhafazası". *Hacettepe Hukuk Fakültesi Dergisi*, 10/1 (2020): 77-107.

Bergel, Cüneyt. "Bilgisayar Ağları ve Güvenlik". *SAU Fen Bilimleri Enstitüsü Dergisi*. 8/1 (2004): 5-8.

Bük, Alaattin. *Bilişim Alanında Kişisel Verilerin Korunması*. Ankara: Seçkin Yayınları, 2018.

Cahit Cengizhan. "Eavesdropping Attack". Erişim Tarihi 15.01.2025, https://cahitcengizhan.com/eavesdropping-attack/#:~:text=Eavesdropping%20attack%20(ya%20da%20dinleme,hassas%20bilgileri%20elde%20etmeyi%20ama%C3%A7lar

Cambridge Dictionary. "Cambridge Dictionary". Erişim Tarihi 28.02.2025, https://dictionary.cambridge.org/.

Council of Europe. "Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001". Erişim Tarihi 15.01.2025 https://www.coe.int/en/web/cybercrime/the-budapest-convention

CyberMag. "En Yaygın Siber Saldırı Türü: Web Shell En Çok Hedef Alınan Sektör: Sağlık". Erişim Tarihi 15.01.2025, https://www.cybermagonline.com/en-yaygin-siber-saldiri-turu-web-shell-en-cok-hedef-alinan-sektor-saglik

Çakıcı, Mert. "Türk Ceza Kanunu M. 243 ve M. 244'te Düzenlenen Bilişim Suçları". *Ceza Hukuku Dergisi*. 9/24 (2014): 307-349.

Çakır, Hamza ve Hakan Topçu. "Bir İletişim Dili Olarak İnternet". *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi.* 1/19 (2005): 71-96.

Çakır, Hüseyin ve Ercan Sert. "Bilişim Suçları ve Delillendirme Süreci". İçinde *Örgütlü Suçlar ve Yeni Trendler*, editör Oğuzhan Ömer Demir ve Murat Sever, 143-172. Ankara: Polis Akademisi Yayınları, 2011.

Çakmak, Haydar ve Korhan Demir. "Siber Dünyadaki Tehdit ve Kavramlar". İçinde *Terör & Savaş Üçgeninde Siber Dünya*, editör Haydar Çakmak ve Taner Altınok, 23-54. Ankara: Barış Platin Kitabevi ,2009.

Çiçek, Niyazi. "Hukuksal Geçerlilik Bakımından Resmi Belgelerin Biçimsel Özellikleri". *Amme İdare Dergisi*. 40/4 (2007): 133-153.

Danyal, Devrim. “Crowdstrike ve Microsoft güncellemesi nasıl global sistem krizine dönüştü?”. *Anadolu Ajansı.* 19.07.2024. https://www.aa.com.tr/tr/analiz/crowdstrike-ve-microsoft-guncellemesi-nasil-global-sistem-krizine-donustu/3280058

Değirmenci, Olgun. “2004 Türk Ceza Kanunu’nun Bilişim Suçları Bakımından Değerlendirilmesi”. *TBB Dergisi*. 58 (2005): 195-208.

Demir, Ömer, Mehmet Arıç ve Halil Polat. *Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar.* Ankara: Adalet Yayınevi, 2015.

Demiral, Ayşenur. “Dijital Delil Nedir? Ne işe Yarar?”. Erişim Tarihi 02.02.2025, https://www.siberegitmen.com/dijital-delil-nedir/

Demirbaş, Timur. *Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayıncılık, 2023.

Demircan, Tunç. *Bilişim Alanında Suçlar*. İstanbul: Legal Yayıncılık, 2016.

Demirci, Ömer. *Bilişim Suçları ve Soruşturma Yöntemleri*. Ankara: Seçkin Yayınları, 2022.

Demirer, Egemen. “Siber Uzay ve Siber Güvenlik Nedir?”. Erişim Tarihi 15.01.2025. Hukuk ve Bilişim, https://www.hukukvebilisimdergisi.com/siber-uzay-ve-siber-guvenlik/.

BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı. “Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri”. *Bilgi Teknolojileri ve İletişim Kurumu,* (2022). https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/dijitallesen-dunyada-bilisim-suclari-ve-mucadele-yontemleri-6218e2417eaea.pdf

Dokurer, Semih. “Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri”. *İnet-tr 2001* (2003). http://www.dokurer.net/files/documents/Bilisim_Suclari_2001.pdf.

Dursun, Hasan. “Bilgisayar İle İlgili Suçlar”. *Yargıtay Dergisi*. 24/3, (1998): 334-339.

Dülger, Murat Volkan. “Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler”. *İstanbul Barosu Dergisi*. 4 (2004): 1485-1496.

Dülger, Murat Volkan. *Bilişim Suçları.* Ankara: Seçkin Yayınları, 2004.

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku*, Ankara: Seçkin Yayınları, 2023.

Dülger, Murat Volkan. "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık İngiltere Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması". *Türkiye Adalet Akademisi Dergisi*. 31 (2017): 141-258.

Dülger, Murat Volkan ve Onur Özkan. "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi". İçinde *Prof. Dr. Mehmet Emin Artuk'a Armağan*, editör Mahmut Koca, 935-962. Ankara: Seçkin Yayıncılık, 2020.

Efe, Ahmet, Gizem Kalkancı, Mehmet Donk, Serhat Cihangir ve Ziya Uysal. "A Hidden Hazard: Man-In-The-Middle Attack in Networks". *Computer Science*. 4/2 (2019): 96-116.

Egemenoğlu, Alaaddin ve Esra Alan. *Ceza Hukuku Temel Kavramlar*. Ankara: Seçkin Yayıncılık, 2023.

Eker, Ö. Umut. ""Türk Ceza Hukuku'nda Bilişim Suçları"" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu". *Türkiye Barolar Birliği Dergisi*. 19/62 (2006): 101-131.

Ekici, Şerafettin. "Bir İletişim Ortamı Olarak İnternet ve Türkiye'de İnternetin Regülasyonu". Yüksek Lisans Tezi, Marmara Üniversitesi, 2009.

Elbahadır, Hamza. *Hacking Interface.* İstanbul: Kodlab Yayıncılık, 2020.

Eliaçık, Cihad Furkan. *Uluslararası Hukuk Bağlamında Nükleer Santrallerin Siber Güvenliği.* Ankara: Seçkin Yayınları, 2018.

Erdağ, Ali İhsan. "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)". *Gazi Üniversitesi Hukuk Fakültesi Dergisi.* 14/2 (2010): 275-303.

Erdem, Fazıl Hüsnü. "TCK'nun 312. Maddesinin Koruduğu Hukuksal Değerin Kısa Bir Analizi: Türk Devlet Düzeni V. Demokratik Kamu Düzeni". *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 52/1 (2003): 37-62.

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

Erdoğan, Yavuz. “Türk Ceza Kanununda bilişim sistemini engelleme bozma verileri yok etme değiştirme suçu”. Doktora tezi, Marmara Üniversitesi, 2011.

Erdoğan, Yavuz. *Türk Ceza Kanunu’nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*. İstanbul: Legal Yayıncılık, 2012.

Erem, Faruk. “Bilgisayar Suçları ve Türk Ceza Kanunu”. *İstanbul Barosu Dergisi*. 19/10-11-12 (1993): 178-186. https://tbbdergisi.barobirlik.org.tr/m1993-19932-968

Erkan, Gülennur. “Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları”. Yüksek Lisans Tezi, Erciyes Üniversitesi, 2021.

Ermeydan, Damla. *Türk Ceza Kanunu’nda Bilişim Suçları*. Ankara: Seçkin Yayınları, 2023.

Ersoy, Yüksel. “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları”. *Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi*, 49/3 (1994): 149-183.

Ertam, Fatih. “Bilgisayar Ağları Ve İnternet Üzerinden Başka Bir Bilgisayarın Kontrolü”. Yüksek Lisans Tezi, Fırat Üniversitesi, 2005.

Eryiğit, Beyza Melek. “Dolandırıcılık Suçu ve Özel Olarak Bilişim Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması Suretiyle Nitelikli Dolandırıcılık Suçu. Yüksek Lisans Tezi, İstanbul Üniversitesi, 2019.

Fichman, P. & H. Rosenbaum, *Social informatics: Past, present and future*. Newcastle, UK: Cambridge Scholars Publishing, 2014.

Geçmez, İrem. *Bilişim Sistemini Engelleme, Bozma Verileri Yok Etme veya Değiştirme Suçları (TCK M. 244)*. Ankara: Seçkin Yayınları, 2020.

Gemalmaz, Haydar Burak. *Mülkiyet Hakkı*. Ankara: Avrupa Konseyi, 2018.

Gerçeker, Hasan. *Yorumlu ve Uygulamalı Türk Ceza Kanunu*. Ankara: Seçkin Yayıncılık, 2022.

Geyik, Atilla. “Türk Ceza Hukuku’nda Mala Zarar Verme Suçu”. Yüksek Lisans Tezi, Dicle Üniversitesi, 2014.

Gökcan, Hasan Tahsin ve Mustafa Artuç. *Pratik Türk Ceza Kanunu*. Ankara: Adalet Yayınevi, 2023.

Gökçearslan, Şahin. “Bilişim Suçları ve Etik”, İçinde *Eğitimde Bilişim Teknolojileri I-II*, editör Sami Şahin ve Çelebi Uluyol, 127-148. Ankara: Pegem Akademi Yayıncılık,2016.

Görgülü, Eymen. “İnternet’in Öyküsü: Geçmişten Günümüze”. *Bilişim Kültürü Dergisi*. 1/2 (2021): 92-97.

Gözel, Arif. “Belgede Sahtecilik Suçlarının Konusu Olarak Belge ve Elektronik Belge”. *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*. 5/1 (2015): 143–201.

Gözüşirin, Mesih. “5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi”. Yüksek Lisans Tezi, Kara Harp Okulu, 2011.

Gtech. “Nesnelerin İnterneti (IoT) Nedir?”. Erişim Tarihi 15.01.2025, https://www.gtech.com.tr/nesnelerin-interneti-iot-nedir/

Gül, Ahmet. *Doğrudan Dolaylı Bilişim Suçları*. Ankara: Seçkin Yayınları, 2021.

Gümüş, Çetin. “Bilişim Suçlarıyla Mücadelede Polisin Eğitimi”. Doktora Tezi, Fırat Üniversitesi, 2008.

Gün, Nagihan. “Türk Ceza Hukukunda Bilişim Suçları”. Yüksek Lisans Tezi, Çankaya Üniversitesi, 2020.

Gündüz, M. Zekeriya. “Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti”. Yüksek Lisans Tezi, Fırat Üniversitesi, 2013.

Hafızoğulları, Zeki ve Devrim Güngör. “Türk Ceza Hukukunda Suçların Tasnifi”. *Türkiye Barolar Birliği Dergisi,* 69 (2007): 21-50.

Henkoğlu, Türkay ve Özgür Külcü. “Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme”. *Bilgi Dünyası.* 14/1 (2013): 62-86.

İçel, Kayıhan. “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri”. *Journal of Istanbul University Law Faculty*. 59/1-2 (2011): 3-10.

İhtiyaroğlu, Uğur. “Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi”. *Hacettepe Hukuk Fakültesi Dergisi*. 10/2 (2020): 406-440.

İnanıcı, Haluk. “Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü”. *İstanbul Barosu Dergisi*. 70/7,8,9 (1996) : www.inanici-tekcan.av.tr/images/pdf/bilisim-yazilim.pdf

Kaçmaz Keskin, Gözde. *Türk ve Amerikan Hukukunda Tüzel Kişilerin Ceza Sorumluluğu*. Ankara: Seçkin Yayıncılık, 2024.

Kangal, Zeynel T. “Fransa’da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu”. *Journal of Istanbul University Law Faculty*. 59/1-2 (2011): 227-240.

Karagöz, Mehmet Can. “Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)”. Yüksek Lisans Tezi, Akdeniz Üniversitesi, 2019.

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

Karakehya, Hakan. “Türk Ceza Kanununda Bilişim Sistemine Girme Suçu”. *Türkiye Barolar Birliği Dergisi.* 81 (2009). 1-24.

Karipçin, Sümeyra. “Türk Ceza Kanunu’nda Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244/1,2)”. Yüksek Lisans Tezi, Selçuk Üniversitesi, 2019.

Kaspersky. “DDoS Saldırısı Nedir?”. Erişim Tarihi 15.01.2025, https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks

Kaspersky. “Farklı kötü amaçlı yazılım türleri nelerdir?”. Erişim Tarihi 15.01.2025, https://www.kaspersky.com.tr/resource-center/threats/types-of-malware

Kaspersky. “IP Adresi nedir?”. Erişim Tarihi 15.01.2025, https://www.kaspersky.com.tr/resource-center/definitions/what-is-an-ip-address

Kaspersky. “İnternet güvenliği: Nedir ve Çevrimiçiyken Kendinizi Nasıl Koruyabilirsiniz?”. Erişim Tarihi 15.01.2025, https://www.kaspersky.com.tr/resource-center/definitions/what-is-internet-security

Kaspersky. “Rootkit nedir”. Erişim Tarihi 15.01.2025, https://www.kaspersky.com.tr/resource-center/definitions/what-is-rootkit

Kaspersky. “SQL aşılama nedir?”. Erişim Tarihi 15.01.2025, https://www.kaspersky.com.tr/resource-center/definitions/sql-injection

Katoğlu, Tuğrul. “Ceza Hukukunda Suçun Mağduru Kavramının Sınırları” *Atatürk Üniversitesi Hukuk Fakültesi Dergisi.* 61/2 (2012): 657-693.

Kayaer, Nebahat. “Türk Hukukunda Bilişim Sistemine Girme Suçu (TCK. m. 243)”, *Ceza Hukuku Dergisi,* 14/39 (2019): 83-128.

Keser, Hafize. “Bilgisayarın Evrimi”. *Ankara University Journal of Faculty of Educational Sciences (JFES).* 24/2 (1991): 411-422.

Ketizmen, Muammer. “Türk Ceza Hukuku’nda Bilişim Suçları”. Doktora Tezi, Ankara Üniversitesi, 2006.

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

Koca, Mahmut. “Hukukumuzda TCK’nun 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu”. İçinde *Bilişim Hukuku Konferansı,* 89-99. Ankara: Yargıtay Başkanlığı Yayınları, 2009.

Koca, Mahmut ve İlhan Üzülmez. *Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayınları, 2023.

Koca, Mahmut ve İlhan Üzülmez. *Türk Ceza Hukuku Özel Hükümler*. Ankara: Adalet Yayınevi, 2024.

Korkmaz, Fulya. “Dolandırıcılık Suçunun Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi”. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*. 69/3 (2020): 1415-1436.

Köker, Ahmet Emre. “Ulusal Siber Güvenlik Stratejisi: Fransa”. *UPA Strategic Affairs*. 3/1 (2022): 42-78.

Köksal, Aydın. *Bilişim Terimleri Sözlüğü*. Ankara: Türk Dil Kurumu Yayınları, 1981.

Kron Teknoloji. “En Sık Karşılaşılan 10 Siber Saldırı Yöntemi”. Erişim Tarihi 15.01.2025, https://kron.com.tr/en-sik-karsilasilan-10-siber-saldiri-yontemi

Kurt, Levent. *Açıklamalı - İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*. Ankara: Seçkin Yayıncılık, 2005.

Lal, Melisa. “Bilişim Sistemleri Aracılığıyla Haksız Yarar Sağlama Suçu”. Yüksek Lisans Tezi, Yaşar Üniversitesi, 2022.

Mahmutoğlu, Fatih Selami. “Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu”. *Journal of Istanbul University Law Faculty*, 59/1-2 (2011): 39-49.

Mahmutoğlu, Fatih Selami. “Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”. *Journal of İstanbul University Law Faculty.* 71/1 (2013): 855-889.

Malkoç, İsmail. *Açıklamalı – İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu Madde 179-345 2. Cilt.* Ankara: Malkoç Kitabevi Yayınları, 2008.

Maşite Danışman. “Password Attacks”. Erişim Tarihi 15.01.2025, https://www.siberguvenlik.web.tr/password-attacks-sifre-saldirilari/

Nacar, Fatma Burcu. “Avrupa Birliği Ülkeleri ve Türkiye’de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları”. Yüksek Lisans Tezi, Atılım Üniversitesi, 2010.

Niobehosting. “Malware Nedir? Çeşitleri Nelerdir?”. Erişim Tarihi 15.01.2025, https://www.niobehosting.com/blog/malware-nedir/

Niobehosting. SQL Injection Nedir? Nasıl Tespit Edilir? Nasıl Engellenir?”. Erişim Tarihi 15.01.2025, https://www.niobehosting.com/blog/sql-injection/

Önder, Ayhan. *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar*. İstanbul: Filiz Kitabevi, 1994.

Öndin, Hasan Burak. “Türk Hukukunda Doğrudan Bilişim Suçları”. Yüksel Lisans Tezi, Anadolu Üniversitesi, 2017.

Önok, Murat. “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 19/2 (2013): 1229-1270.

Özbek, Veli Özer. “Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)”. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*. 9/Özel Sayı (2007): 1019-1063.

Özbek, Veli Özer. “İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları”. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*. 4/1, (2002): 101-158.

Özbek, Veli Özer vd. *Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayınları, 2023.

Özbek, Veli Özer, Koray Doğan ve Pınar Bacaksız. *Türk Ceza Hukuku Özel Hükümler.* Ankara: Seçkin Yayınları, 2023.

Özen, Muharrem ve Gürkan Özocak. "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)". *Ankara Barosu Dergisi,* 1 (2015): 41-77.

Özgenç, İzzet ve İlhan Üzülmez. *Temel Hukuk Dizisi Ceza Genel Hukuku*. Ankara: Seçkin Yayıncılık, 2022.

Özgenç, İzzet. *Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayıncılık, 2024.

Özkul, Davut. "Bilişim Sistemi Kavramı Ve Bilişim Sistemlerinin Denetimi". *Sayıştay Dergisi.* 13/44-45 (2002): 11-34.

Öztekin, Alp. *Bilişim Sistemine Girme Suçu.* Ankara: Seçkin Yayınları, 2023.

Öztemiz, Semanur. "Sosyal Bilişim Üzerine Kavramsal Bir Değerlendirme". *Bilişim Teknolojileri Dergisi.* 11/ 4 (2018): 309-319.

Özsoy, Nevzat. "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK 243 ve 244)", *Yaşar Hukuk Dergisi,* 1/2 (2019): 295-352.

Özüdoğru, Uğur. "Siber Suçlar ve Mücadele Yöntemleri Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri". Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, 2011.

Pallı, Hayati. "Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları". Yüksek Lisans Tezi, Erciyes Üniversitesi, 2008.

Pancaroğlu, Başar. "Bilişim Sistemlerindeki Veriler Bağlamında Belgede Sahtecilik Suçu". Yüksek Lisans Tezi, Hacı Bayram Veli Üniversitesi, 2019.

Parlar, Ali. *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Sage Yayıncılık, 2014.

Polat, Emre. "Yargı Kararları Işığında Mala Zarar Verme Suçu". Yüksek Lisans Tezi, Selçuk Üniversitesi, 2023.

Raufoğlu, Tabriz. *Hukuki Yönleri ile Siber Alanda Yetki Sorunu*. Ankara: Adalet Yayınevi, 2022.

Sarıgül, Ali Tanju. "Bilişim Teknolojisinde Bir Suistimal Örneği: Bilişim Sistemlerinin Kullanılması Suretiyle Dolandırıcılık Suçları". İçinde *Bilişim ve Teknoloji Yıllığı 2022*. editör Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar. 90-100. Ankara: Adalet Yayınevi, 2022.

Sarıtaş, Erkan. "Cezalandırılmayan Önceki Hareketler", *İstanbul Hukuk Mecmuası*. 80/2 (2022): 615-654. 10.26650/mecmua.2022.80.2.0008 https://dergipark.org.tr/pub/ihm http://mecmua.istanbul.edu.tr/tr/

Sarsıkoğlu, Şenel. "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı". *Türkiye Adalet Akademisi Dergisi*, 22 (2015): 427-454.

Sarsıkoğlu, Şenel. "Halkı Yanıltıcı Bilgiyi Alenen Yayma (Dezenformasyon) Suçu (TCK m. 217/A)". *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, 7/3 (2024): 720-755.

Sarzana, Carlo. "Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması İtalya'daki Durum". çev. Vesile Sonay Daragenli. *İstanbul Hukuk Fakültesi Dergisi*. LV/3 (1997): 389-405.

Serin, Hüseyin. "Ergenlerde Siber Zorbalık/ Siber Mağduriyet Yaşantıları ve Bu Davranışlara İlişkin Öğretmen ve Eğitim Yöneticilerinin Görüşleri". Doktora Tezi, İstanbul Üniversitesi, 2012.

Sieber, Ulrich. "Bilişim Suçları". İçinde *Bilişim Teknolojisi İle Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku (Yazarın Seçilmiş Makaleleri)*, editör, Feridun Yenisey, Salih Oktar, Zehra Başer Doğan, 259-302. Ankara: Seçkin Yayıncılık, 2021.

Sokullu Akıncı, Füsun. "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi". *Journal of Istanbul University Law Faculty*. 59/1-2 (2011): 11-38

Solmaz, Saltuk Buğra. "Siber Güvenlik Tarihindeki Dönüm Noktaları: Tehditlerin Evrimi ve Savunma Stratejileri". *Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve Uygulama Merkezi Dergisi*. 3/1 (2023): 1-9.

Soyaslan, Doğan. *Ceza Hukuku Özel Hükümler*. Ankara: Yetkin Yayınları, 2016.

STM ThinkTech. "Siber Tehdit Durum Raporu (Ocak-Mart 2018)", https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2018.

STM ThinkTech. “Siber Tehdit Durum Raporu (Ocak-Mart 2024)”, https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2024.

Sunay, Reyhan. “Avrupa Sözleşmesi Çerçevesinde Oluşan "Avrupa Kamu Düzeni" Kavramının Kapsamı ve Fonksiyonel Değeri”. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 7/1-2 (1999): 309-330.

Sütçü, Cem S. “Bilgisayar ve Bilgisayar Ağları”. *Marmara İletişim Dergisi*. 5/5 (1994): 145-152.

Şamlı, Rüya. “Türk ve Dünya Hukukunda Bilişim Suçları”. içinde *Akademik Bilişim ’10 XII. Akademik Bilişim Konferansı Bildirileri*, editör Mustafa Akgül, Ethem Derman, Ufuk Çağlayan, Atilla Özgit, Tuğrul Yılmaz, 121-128. Muğla: Muğla Üniversitesi, 2010.

Şamlıoğlu, Hamza. “Ağ İletişim Protokolleri ve Portlar”. Erişim Tarihi 15.01.2025, https://www.priviasecurity.com/ag-iletisim-protokolleri-ve-portlar/

Şimşek, Altın Aslı. “Genel Kamu Hukukunun Temel Kavramı Olarak Kamu Düzeni”. Yüksek Lisans Tezi, Ankara Üniversitesi, 2010.

Taşdemir, Kubilay. *Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları.* Ankara: Ütopyagrafik, 2009.

Taşkın, Ahmet ve İbrahim Zengin. *Ceza Hukuku El Kitabı.* Ankara: Seçkin Yayıncılık, 2004.

Taşkın, Ş. Cankat. “Bilişim Hukuku Uluslararası Uyuşmazlıklar”. *TBB Dergisi*. 85 (2009): 332- 372. http://tbbdergisi.barobirlik.org.tr/m2009-85-571

Taşkın, Şaban Cankat. “Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları”. Yüksek Lisans Tezi, Marmara Üniversitesi, 2008.

Taşkın, Şaban Cankat. “Stalking (Siber Gözetlenme) Eyleminin Ceza Hukukundaki Yaptırımının Değerlendirilmesi”. İçinde *Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı*, editör Şerafettin Ekici, Ekrem Solak ve Muhammed Emre Avşar, 289-312. Ankara: Adalet Yayınevi, 2021.

Tekin, Nurullah. “Resmi Belgede Sahtecilik Suçunda Bazı Özel Durumlar”. *Türkiye Adalet Akademisi Dergisi*. 5/19 (2014): 903-941.

Tepe, İlker. “İnternet ve Ceza Hukuku – Modern Ceza Hukuku Teorisinde İnternet ve İnternet Suçluluğunun Konumu”. *Ceza Hukuku Dergisi*. 4/9 (2009): 259-272.

Tezcan, Durmuş, Mustafa Ruhan Erdem ve Murat Önok. *Teorik ve Pratik Ceza Özel Hukuku*. Ankara: Seçkin Yayıncılık, 2023.

Tulum, İsmail. "Bilişim Suçlarıyla Mücadele". Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, 2006.

Turan, Metin. *Bilişim Hukuku*. Ankara: Seçkin Yayınları, 2023.

Turan, Metin. *Bulut Bilişim*. Ankara: Seçkin Yayınları, 2019.

Turan, Metin ve Özgür Külcü. "Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi". *Türk Kütüphaneciliği*. 28/1 (2014):18-46.

Turhan, Çağda Nur. "Resmi Belgede Sahtecilik Suçu". Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi, 2016.

Turhan, Oğuz. "Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar)". Planlama Uzmanlığı Tezi, TC. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, 2006.

Turhost. "Ortadaki Adam (MitM) Saldırısı Nedir?". Erişim Tarihi 15.01.2025, https://www.turhost.com/blog/ortadaki-adam-mitm-saldirisi-nedir/#serp

Turhost. "SQL Injection Nedir?". Erişim Tarihi 15.01.2025, https://www.turhost.com/blog/sql-injection-nedir/#serp

Turk.Net. "IP (İnternet Protokolü) Nedir?". Erişim Tarihi 15.01.2025, https://turk.net/blog/ip-internet-protokolu-nedir/#:~:text=IP%20adresleri%2C%20internete%20ba%C4%9Flanmak%20isteyen,siber%20g%C3%BCvenlik%20konular%C4%B1nda%20da%20kullan%C4%B1l%C4%B1r

Türk Dil Kurumu. "Türk Dil Kurumu sözlüğü". Erişim Tarihi 15.01.2025, https://sozluk.gov.tr/

Türkiye Büyük Millet Meclisi. "Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu (1/593)". Erişim Tarihi 15.01.2025, https://cdn.tbmm.gov.tr/KKBSPublicFile/D22/Y1/T1/DosyaKomisyonRaporunuVerdi/08f04456-d914-428b-8ee5-49694952fd88.htm

Uçak, Nazan Özenç. "Bilgi: Çok Yüzlü Bir Kavram". *Türk Kütüphaneciliği Dergisi*, 24/4 (2010): 705-722.

Uçak, Nazan Özenç. "Bilgi Üzerine Kuramsal Bir Yaklaşım". *Bilgi Dünyası Dergisi*, 1/1 (2000): 143-159.

Uçar, Hüdaverdi. "5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları". Yüksek Lisans Tezi, Çankaya Üniversitesi, 2014.

USCA Second Circuit, United States of America, Appellee, v. Robert Tappan Morris, 07.03.1991, Appl. No. 774, Docket 90-1336. https://scholar.google.com/scholar_case?case=551386241451639668

Ünver, Yener. "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi", *Journal of İstanbul University Law Faculty*, 59/1-2 (2011): 51-153.

Wolcott, Peter and Kursat Çağıltay, "Telecommunications, Liberalization, and the Growth of The Internet in Turkey". *Information Society.* 17/2 (1999): 133-141.

Wolcott, Peter. "The Diffusion Of The Internet In The Republic Of Turkey". *University of Nebraska.* (1999).

Yargıtay 2. Ceza Dairesi. K. 2016/10421 (01 Haziran 2016) https://karararama.yargitay.gov.tr/.

Yargıtay 5. Ceza Dairesi. K. 2014/7366. (03 Temmuz 2014) https://karararama.yargitay.gov.tr/

Yargıtay 6. Ceza Dairesi. K. 2008/12249. (02 Haziran 2008) https://karararama.yargitay.gov.tr/

Yargıtay 8. Ceza Dairesi. K. 2014/17639. (07 Temmuz 2014) https://karararama.yargitay.gov.tr/

Yargıtay 8. Ceza Dairesi. K. 2014/ 18506. (14 Temmuz 2014) https://karararama.yargitay.gov.tr/

Yargıtay 8. Ceza Dairesi. K. 2015/14023 (18 Mart 2015). https://karararama.yargitay.gov.tr/

Yargıtay 8. Ceza Dairesi. K. 2016/8047. (16 Haziran 2016) https://karararama.yargitay.gov.tr/

Yargıtay 8. Ceza Dairesi. K: 2017/175 (11 Ocak 2017) https://karararama.yargitay.gov.tr/,

Yargıtay 8. Ceza Dairesi. K. 2018/4133. (12 Nisan 2018). https://karararama.yargitay.gov.tr/.

Yargıtay 8. Ceza Dairesi. K. 2018/560. (18 Ocak 2018). https://kazanci.com.tr/.

Yargıtay 8. Ceza Dairesi. K. 2022/4436. (15 Mart 2022) https://karararama.yargitay.gov.tr/

Yargıtay 8. Ceza Dairesi. K. 2022/912. (19 Ocak 2022) https://karararama.yargitay.gov.tr/

Yargıtay 11. Ceza Dairesi. K. 2009/11328, (07 Ekim 2009) https://karararama.yargitay.gov.tr/.

Yargıtay 11. Ceza Dairesi. K. 2007/5533, (18 Eylül 2007). www.kazanci.com.tr.

Yargıtay 11. Ceza Dairesi. K. 2009/101. (28 Ocak 2009). https://kazanci.com.tr/.

Yargıtay 11. Ceza Dairesi. K. 2013/4065. (13 Mart 2013) https://karararama.yargitay.gov.tr/.

Yargıtay 11. Ceza Dairesi. K. 2019/2115 (28 Şubat 2019) https://karararama.yargitay.gov.tr/.

Yargıtay 11. Ceza Dairesi. K. 2021/2806. (18 Mart 2021) https://karararama.yargitay.gov.tr/

Yargıtay 12. Ceza Dairesi, K. 2014/17770 (15 Eylül 2014) https://karararama.yargitay.gov.tr/.

Yargıtay 12. Ceza Dairesi. K. 2017/1556. (01 Mart 2017) https://kazanci.com.tr/.

Yargıtay 12. Ceza Dairesi. K. 2017/7642. (18 Ekim 2017) https://karararama.yargitay.gov.tr/

Yargıtay 13. Ceza Dairesi. K. 2017/10403. (10 Ekim 2017) https://karararama.yargitay.gov.tr/.

Yargıtay 15. Ceza Dairesi. K. 2018/1367. (27 Şubat 2018). https://kazanci.com.tr/

Yargıtay 23. Ceza Dairesi. K. 2016/6542 (24 Mayıs 2016). https://kazanci.com.tr/

Yargıtay Ceza Genel Kurulu. K. 2000/72 (11 Nisan 2000). https://kazanci.com.tr/

Yargıtay Ceza Genel Kurulu. K. 2008/150. (27 Mayıs 2008). https://karararama.yargitay.gov.tr/

Yargıtay Ceza Genel Kurulu. K. 2007/150. (19 Haziran 2007). https://karararama.yargitay.gov.tr/.

Yargıtay Ceza Genel Kurulu. K. 2008/92. (29 Nisan 2008). https://kazanci.com.tr/

Yargıtay Ceza Genel Kurulu. K. 2009/268 (17 Kasım 2009). www.kazanci.com.tr

Yargıtay Ceza Genel Kurulu. K. 2009/268 (17 Kasım 2009). https://kazanci.com.tr/

Yargıtay Ceza Genel Kurulu. K. 2010/65. (30 Mart 2010) https://karararama.yargitay.gov.tr/

Yargıtay Ceza Genel Kurulu. K. 2017/13. (17 Ocak 2017). https://kazanci.com.tr/.

Yargıtay Ceza Genel Kurulu. K. 2017/27 (24 Ocak 2017) https://karararama.yargitay.gov.tr/

Yargıtay Ceza Genel Kurulu. K. 2020/381. (29 Eylül 2020). https://karararama.yargitay.gov.tr/.

Yargıtay Ceza Genel Kurulu. K. 2021/68 (02 Mart 2021). https://kazanci.com.tr/

Yargıtay Hukuk Genel Kurulu. K. 2023/408. (03 Mayıs 2023). https://kazanci.com.tr/

Yaşar, Osman, Hasan Tahsin Gökcan ve Mustafa Artuç. *Yorumlu – Uygulamalı Türk Ceza Kanunu*. Ankara: Adalet Yayınevi, 2014.

Yaycı, Esra. "Bilişim Suçları". Yüksek Lisans Tezi, Gazi Üniversitesi, 2007.

Yazıcı, Necmettin. "Türk Ceza Hukukunda Bilişim Suçları (TCK M. 243-244 ve 245)". Yüksek Lisans Tezi, Fatih Sultan Mehmet Vakıf Üniversitesi, 2021.

Yazıcıoğlu, Yılmaz. "Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı". İçinde *Uluslararası İnternet Hukuku Sempozyumu*, 451-470. İzmir: Dokuz Eylül Üniversitesi Yayını, 2002.

Yazıcıoğlu, Yılmaz. *Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle*. İstanbul: Alfa Yayınları, 1997.

Yazıcıoğlu, Yılmaz. "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi". İçinde *Yeni Türk Ceza Kanunu Sempozyumu*. İstanbul: Türk Ceza Hukuku Derneği Yayını, 2005.

Yazıcıoğlu, Recep Yılmaz. "Hukukumuzda TCK'nun 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi". İçinde *Bilişim Hukuku Konferansı*, 69-87. Ankara: Yargıtay Başkanlığı Yayını, 2009.

Yenidünya, Ahmet Caner. “Bilişim Sistemine Hukuka Aykırı Erişim Suçu”. *Fikri ve Sınai Haklar Dergisi*, 4 (2005) : 1017-1042.

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

Yetim, Servet. “Bilişim Suçları ve Etkin Mücadele Yöntemleri”. *Terazi Hukuk Dergisi*. 9/95 (2014) : 80-86.

Yıldız, Mehmet Emre. “İnternet Bankacılığı Hakkında Yargıtay’ın 17.11.2009 Tarih, 2009/11-193 Esas Sayılı Kararının İncelenmesi”. *Ceza Hukuku Dergisi*. 5/14 (2010): 129-150.

Yıldız, Özcan Rıza. “Bilişim Dünyasının Yeni Modeli: Bulut Bilişim (Cloud Computing) ve Denetim”. *Sayıştay Dergisi*. 74 (2009) : 5-23.

Yılmaz, Sacit. “5237 Sayılı TCK’nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar”. *TBB Dergisi*, 92 (2011), 62-100.

Yılmaz, Sacit. *Türk Ceza Hukuku Sisteminde Siber Suçlar*. Ankara: Adalet Yayınevi, 2023.

Yılmaz, Furkan ve Fuat Güllüpınar. “Türkiye’de Bilişim suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi”, *Uluslararası Toplum Araştırmaları Dergisi*, 15/10 (2020), 5371-5409.

Yılmaz, Malik. “Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi Ve Bilgi Yönetimi”, *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49/1 (2009): 95-118.

Yüksektepe, Mert Asker. *Bilişim Suçları ve Soruşturma Usulü*. İstanbul: Platon Plus Yayıncılık, 2022.