ÇANKAYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU YÜKSEK LİSANS TEZİ

TÜRK CEZA HUKUKUNDA BİLİŞİM SUÇLARI

NAGİHAN GÜN

HAZİRAN 2020

ÖZET

TÜRK CEZA HUKUKUNDA BİLİŞİM SUÇLARI

GÜN, Nagihan
Yüksek Lisans Tezi
Kamu Hukuku Anabilim Dalı

Tez Danışmanı: Doç. Dr. Elvan KEÇELİOĞLU
Haziran 2020, 355 sayfa

Bilginin işlenmesi ve yönetilmesinde hız ve kolaylık sağlayan bilişim sistemleri bireylerin özel yaşamından kamu kurumlarının veya özel kuruluşların yürüttüğü hizmetlere kadar kullanılması sonucunu doğurup hayatımızın neredeyse her alanına nüfuz ederek kullanım payını yadsınamayacak oranda genişletmiştir. Bilişim sistemlerinin günümüz dünyasının vazgeçilmez unsurları olduğu göz önüne alındığında bu sistemler aracılığıyla gerçekleştirilen ihlallerin de gecikmeksizin, hızlı, öngörülü bir şekilde çözüme kavuşturulması ve oluşturulacak maddi ceza normlarının da değişen çağa uyum sağlayabilecek kapsamda düzenlenmesi gerekmektedir. Bilişim alanının sınırlarının olmaması karşısında bu alanda işlenen suçlarla etkili mücadelede sadece ülkelerin ulusal mevzuatlarında yer alan düzenlemelerin yeterli olmayacağı açıktır. Dolayısıyla, söz konusu suçlarla mücadelede ortak dilin oluşturulması ve ulusal yasal mevzuatların birbirlerine uyumlu hale getirilmeleri gerekmektedir. Bu bağlamda çalışmamızın, Türk Ceza Kanunu'nda bilişim alanında suçlar hakkında yer alan mevcut düzenlemeler, bu düzenlemelerin mukayeseli hukukla uyumu, düzenlemelerde eksiklik bulunan yönlerinin değerlendirilmesi ve öneriler getirilmesi suretiyle bu alana katkı sağlayabilecek nitelikte bir çalışma olması hedeflenmektedir.

Çalışmamızda 5237 sayılı Türk Ceza Kanunu'nun (TCK) "Bilişim Alanında Suçlar" bölümünde yer alan suç tipleri, çeşitli ve sayıca fazla olan kaynak araştırması le birlikte doktrinde yer alan fikirler ve Yargıtay kararları ile zenginleştirilerek maddi ceza hukuku boyutu ile incelenecektir. Bu bağlamda, çalışma konumuzu oluşturan bilişim alanında suçların (dar anlamda bilişim suçları) suçun unsurları esas alınarak incelemesine geçilmeden önce bilişim suçlarına ilişkin temel ve teknik terim ve kavramlar incelenerek bilişim suçlarına özgü genel bilgiler verildikten sonra bilişim suçlarına ilişkin mukayeseli hukukta yer alan düzenlemeler hakkında bilgi verilecektir.

Anahtar Kelimeler: Bilişim, Bilişim Sistemi, Bilişim Suçları, Bilişim Alanında Suçlar, Siber Güvenlik, Siber Terörizm.

ABSTRACT

IT CRIMES IN TURKISH CRIMINAL LAW

GÜN, Nagihan
Master's Thesis
Departmanent of Public Law

Supervisor : Doç. Dr. Elvan KEÇELİOĞLU
June 2020, 355 pages

Information systems that provide speed and convenience in the processing and management of information have resulted in an undeniable share of use by penetrating almost every area of our lives, resulting in the use of individuals from their own lives to services run by private or public institutions. Considering that information systems are indispensable elements of today's world, the violations made through these systems should be resolved in a fast, predictive way and the material punishment norms to be created should be arranged in a scope that can adapt to the advancing technology. It is clear that only the regulations in the national legislation of the countries will not be enough to struggle the crimes committed in the field of informatics effectively. Therefore, a common language should be established in the struggle against these crimes and national legal regulations should be harmonized. In this context, our study aims to contribute to this field by combination of the existing regulations in the field of informatics in the Turkish Penal Code and the harmonization of these regulations with comparative law, as well as evaluation of the deficiencies in such regulations and offering suggestions.

In our study, the types of crime in the "Crimes in the Field of Informatics" section of the Turkish Penal Code numbered 5237 will be examined with the various and numerous resource researches, and the ideas in the doctrine will be enriched by the decisions of the Supreme Court and will be examined in terms of the material

criminal law. In this context, before going to the examination of the crimes based on the elements of the crime in the field of informatics, the basic concepts and technical terms related to the informatics crimes will be examined and general information peculiar to the informatics crimes will be given.

Keywords: Informatics, Information System, Informatics Crimes, Crimes in Field of Informatics, Cyber Security, Cyber Terrorism.

TEŞEKKÜR

Bu çalışmalarım sırasında; değerli vaktini esirgemeden sorularımı hiçbir zaman cevapsız bırakmayan, gelecekteki meslek hayatımda örnek aldığım, tez çalışması sürecinde yardım ve katkıları ile beni bilgilendiren ve yönlendiren tez danışmanım Doç. Dr. Elvan KEÇELİOĞLU' na, çalışmalarım esnasında benden yardım ve desteklerini esirgemeyen değerli mesai arkadaşım Bilişim Uzmanı Gökhan USTA' ya ve manevi destekleriyle beni hiçbir zaman yalnız bırakmayan aileme ve tüm arkadaşlarıma teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa no

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AAK	: Ağ Arayüz Kartı
AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
A.e.	: Aynı eser
A.g.e.	: Adı geçen eser
AİS	: Ağ İşletim Sistemi
AK	: Avrupa Konseyi
AKSS	: Avrupa Konseyi Siber Suç Sözleşmesi
ANS	: Advance Network Services - İleri Ağ Hizmetleri
ARPA	: Advanced Research Project Agency - İleri Düzey Araştırma Projeleri Kurumu
ARPANET	: The Advanced Research Projects Agency Network – Gelişmiş Araştırma Projeleri Dairesi Ağı
APT	: Advanced Persistent Threat - Gelişmiş Kalıcı Tehdit
BIOS	: Basic Input/Output System - Temel Giriş/Çıkış Birimi
BİS	: Bilgi ve İletişim Sistemleri
BİT	: Bilgi ve İletişim Teknolojileri
BKKK	: Banka Kartları ve Kredi Kartları Kanunu
BM	: Birleşmiş Milletler
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CCPCJ	: The Commission on Crime Prevention and Criminal Justice- Suç Önleme ve Ceza Adaleti Komisyonu
CDPC	: Council of Europe European Committee on Crime Problems - Avrupa Konseyi Suç Sorunları Komitesi
CFFA	: Computer Fraud and Abuse Act – Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Yasası
CPU	: Central Processing Unit - Merkezi İşletim Ünitesi

C-PROC	: Cybercrime Programme Office – Siber Suçlar Programı Ofisi
DOS	: Denial of Service- Hizmeti Engelleme Saldırısı
DDOS	: Distributed Denial of Service- Dağıtık Hizmeti Engelleme Saldırısı
EBİ	: Elektronik Bilgi İşlem
EC3	: European Cybercrime Centre - Avrupa Siber Suçlar Merkezi
EJCN	: European Judicial Cybercrime Network - Avrupa Yargı Siber Suç Ağı
ENISA	: European Network and Information Security Agency – Avrupa Ağ ve Bilgi Güvenliği Ajansı
EUCTF	: European Cybercrime Task Force - Avrupa Siber Suç Görev Timi/Gücü
EUROJUST	: European Agency for the Enhancement of Judicial Cooperation - Avrupa Adli İşbirliğinin Geliştirilmesi Ajansı
EUROPOL	: European Police Office - Avrupa Polis Teşkilatı
ET.	: Erişim Tarihi
FTP	: File Transfer Protocol - Dosya Transfer Protokolü
GCA	: Global Cybersecurity Agenda- Küresel Siber Güvenlik Gündemi
GCHQ	: Government Communications Headquarters - Devlet İletişim Merkezi
GDPR	: General Data Protection Regulation - Genel Veri Koruma Yönetmeliği
GST	: Gelişmiş Sürekli Tehdit
G8	: Group of Eight- Sekizler Grubu
HTTP	: Hyper Text Transfer Protocol - Üstün Metin Transfer Protokolü
ICMP	: Internet Control Message Protocol - İnternet Kontrol Mesaj Protokolü
INTERPOL	: International Criminal Police Organization - Uluslararası Kriminal Polis Teşkilatı

IOCTA	: Internet Organised Crime Threat Assessment - İnternet Organize Suç Tehdidi Değerlendirmesi
IoT	: Internet of Things - Nesnelerin İnterneti
IP	: Internet Protocol - İnternet Protokolü
IPA	: Instrument for Pre-accession Assistance - Katılım Öncesi Mali Yardım Aracı
IPSec	: Internet Protocol Security – İnternet Protokol Güvenliği
ISO	: International Standards Organization - Uluslararası Standartlar Organizasyonu
ITU	: International Telecommunication Union - Uluslararası Telekomünikasyon Birliği
KVKK	: Kişisel Verilerin Korunması Kanunu
LAN	: Local Area Network - Yerel Alan Ağı
m.	: Madde
MIT	: Massachusetts Institute of Technology
MODEM	: Modülatör - DEModülatör
NAP	: Network Access Point - Ağ Erişim Noktası
NATO	: North Atlantic Treaty Organization - Kuzey Atlantik Antlaşması Örgütü/ İttifakı
NIS	: Network and Information Security - Ağ ve Bilgi Güvenliği
NSF	: National Science Foundation - (Amerikan) Ulusal Bilim Vakfı
NSFNET	: National Science Foundation Network – Ulusal Bilim Vakfı Ağı
OECD	: Organisation for Economic Co-operation and Development- Ekonomik Kalkınma ve İşbirliği Örgütü
OSI	: Open Systems Interconnection – Açık Sistemler Ara Bağlantısı
PCH	: Platform Controller Hub
RAM	: Random Access Memory - Rastgele Erişilebilen Bellek
ROM	: Read Only Memory – Salt Okunur Bellek
SCADA	: Supervisory Control and Data Acquisition - Merkezi

	Denetleme Kontrol ve Veri Toplama Sistemi
SMTP	: Simple Mail Transfer Protocol - Elektronik Posta Gönderme Protokolü
SSL	: Secure Sockets Layer - Güvenli Soket Katmanı
TCK	: Türk Ceza Kanunu
TCP	: Transmission Control Protocol - İletişim Kontrol Protokolü
TCP/IP	: Transmission Control Protocol/Internet Protocol – Gönderim Kontrol İletişim Kuralı/İnternet İletişim Kuralı
T-CY	: Cybercrime Convention Committee - Siber Suçlar Konvansiyon Komitesi
TDK	: Türk Dil Kurumu
TELNET	: Telecommunication Network - Telekomünikasyon Ağı
TİB	: Telekomünikasyon İletişim Başkanlığı
TMK	: Terörle Mücadele Kanunu
TMRC	: Tech Model Railroad Club
t.y.	: Basım tarihi yok
UDP	: User Datagram Protocol - Kullanıcı Veribloğu İletişim Kuralları
UNODC	: United Nations Office on Drugs and Crime - Birleşmiş Milletler Uyuşturucu ve Suç Ofisi
USOM, TR-CERT	: Ulusal Siber Olaylara Müdahale Merkezi
vb.	: Ve Benzeri
v.d.	: Ve Diğerleri
VPN	: Virtual Private Network – Sanal Özel Ağ
WAN	: Wide Area Network - Geniş Alan Ağı
WLAN	: Kablosuz Yerel Alan Ağları
WWW	: World Wide Web - Geniş Dünya Ağı
y.y.	: Basım yeri yok

GİRİŞ

20. yüzyılın başlarında yaşanan endüstri devriminin temel itici gücü olan enerji ve ulaşım teknolojileri, bugün yerini bilişim teknolojilerine bırakmış durumdadır.[1] Bilişim teknolojileri ve sunmuş dijital teknolojiler, bu teknolojilerin kurmuş olduğu bilişim sistemleri aracılığıyla bilgiye hızlı ve kolay ulaşım ve aktarımın sağlanması sonucunda bireylerin hayatında neredeyse vazgeçilmez unsur olarak yerini almıştır. Modern teknoloji sayesinde hızla ilerleyen ağlar arası iletişimin artması ile bireyleri bir nevi ağ toplumuna dönüştürmüş, bilginin işlenmesi ve yönetilmesinde hız ve kolaylık sağlayan bilişim sistemleri ise bireylerin özel yaşamından kamu kurumlarının veya özel kuruluşların yürüttüğü hizmetlere kadar kullanılması sonucunu doğurup hayatımızın neredeyse her alanına nüfuz ederek kullanım payını yadsınamayacak oranda genişletmiştir. Bugün ise nesnelerin interneti (IoT- Internet of Things), akıllı robotlar, akıllı sistemler, simülasyon, sanal gerçeklik, bulut teknolojisi, 3D, mobil cihaz teknolojileri gibi teknolojiler sayesinde bilişim sistemi olarak kabul edilebilecek yeni sistemler de hayatımıza girmeye devam etmektedir. Günümüz dünyasında bağımlı hale geldiğimiz bilişim sistemlerinin güvenliğinin sağlanamaması halinde ise hem bireylerin hem de toplumun genelinin büyük risklerle karşı karşıya kalma ihtimali bulunmaktadır.

Teknolojik gelişmeler sağladığı faydaların yanında yeni ihlal sahalarını da beraberinde getirmiş, yeni suç ve suçluluk türlerine de sebebiyet vermiştir.[2] Zira, modern teknoloji beraberinde güvenlik sorunlarını da getirerek bilişim sistemlerinin kontrol mekanizmasındaki eksikler, anonimlik gibi haiz olduğu suç yaratıcı özelliklerin de etkisiyle bilişim alanının suçlular açısından keşfedilmesi sonucunu doğurarak yeni ihlal türlerini başka bir deyişle daha önce ülke mevzuatları içerisinde yer almayan kendine özgü yeni ve ayrı suç tiplerini de ortaya çıkarmıştır.

1 Kemal Cılız, "Bilişim Teknolojisinde Gelişmeler", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. bs., Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, 2006, ss. 246-248, s. 246.

2 Levent Kurt, *Açıklamalı - İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* Seçkin Yayıncılık, Ankara, 2005, s. 53.

Endüstri toplumunun yerini alan bilgi toplumu çağının yaşandığı günümüzde bilişim sistemlerinin kullanımı sonucu ortaya çıkan veri miktarındaki artış bunun yanında artan veri trafiği ise "siber saldırgan" olarak da nitelendirilen suç faillerinin yeni hedefi haline gelerek dijital sistemleri hedef alan tehdit ve saldırıların artmasına sebebiyet vermiştir. Bunun yanında bilişim sistemlerinin özellikle enerji, haberleşme, su kaynakları, tarım, sağlık, ulaşım, eğitim, finans gibi kritik altyapı sektörlerinde kullanımı ülke güvenliği ile eş değer anlam taşıdığı benimsenen siber güvenlik kavramının önemini ortaya çıkarmıştır. Bilişim suçlarının siber terörle anılmasının arttığı günümüzde ise devletler sanal ağlar tarafından oluşturulan "kritik altyapılar" ın (yerleşkelerin, ağların, servislerin veya yapıların) yok edilmesi veya işleyişinin aksatılmasının sağlık, kamu düzeni, güvenlik veya bireylerin ekonomik iyiliği, devletin fonksiyonlarının etkinliği üzerinde ciddi etki ve tehlikeleri olabileceği hususuna hassasiyet göstermeye başlamışlardır.[3] Ülkeler açısından kritik niteliğe haiz bu hizmetlerin terör örgütlerinin yeni hedefi haline gelmesi ise ülkeleri ciddi güvenlik tehditleri ile karşı karşıya bırakarak güvenlik açısından mücadele edilecek yeni bir sahayı ortaya çıkarmıştır. Birbirine ağlarla bağlı günümüz dünyasında siber alan veya uzayda devletlerin hakimiyetlerini kaybetme riskinin yanında sınırları da tartışılır hale gelmiştir. Zira, üzerinde merkezi bir otoritenin bulunmadığı bu alanda kötüye kullanımların engellenmesi veya bunlarla mücadele eskisinden çok daha zor hale gelmiştir. Gerçekleştirilecek bir siber saldırı sonucunda ordu haberleşme sisteminin etkilenebileceği, kentin bütün trafik ışıklarını durdurulabileceği, telefonların felç edebileceği, elektrik ve doğalgazın kapatabileceği, bilgisayar sistemlerinin karmaşık hale getirebileceği, ulaşım ve su sistemlerinin çalışamaz hale getirilebileceği, bankacılık ve finans sektörünün çökertebileceği, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasının engelleyebileceği, hükümet kurumlarının alt üst edebileceği, sistemin birden durmasına neden olabileceği senaryo ve tehditleri öngörülebilir bir hal almaya başladığı çağımızda terörizmin yeni bir yüzü olarak yansıyan siber terör ile birlikte savaşların ve terörizmin de şekli ve metodu yeni bir hal almış ve devletlerin siber alan veya siber uzayı yeni bir güvenlik sahası olarak kabul etmesine, esasen birbirinden ayrı olarak düşünülemeyecek olan siber güvenlik, kritik altyapılar ve siber

3 Murat Volkan Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması*", Türkiye Adalet Akademisi Dergisi,* Sayı:31, Yıl:8, Temmuz 2017, ss. 141-256, s. 155.

terörizm konularında teknik ve hukuki boyutları ile bir bütün olarak disiplinler arası çalışmalarını artırmaları sonucunu doğurmuştur.

Modern teknolojinin hızlı gelişiminin korunan hukuki menfaati ihlal eden ve haksızlık niteliği taşıyan fiilleri suç olarak belirleyip yaptırım altına alan maddi ceza hukukuna yansıması ise öteden beri var olan klasik suç tiplerinin bilişim sistemleri ile işlenebilmesi halinin yanında daha önce mevcut olmayan yeni suç tiplerini ortaya çıkarmasıdır. Ancak kıyas yasağı bulunan ceza hukukunda, teknolojinin gelişimi ile birlikte ortaya çıkan yeni haksız müdahaleler ve ihlallerin de öngörülü ve kapsamı geniş tutularak düzenlemeler yapılmasına ihtiyaç duyulmaktadır. Zira, ceza hukukunda mevcut olan bir boşluk toplumsal düzeni derinden etkileyebilecek nitelikte olabilecek kıyas yasağı ile suç olarak düzenlenmiş olan bir norm yeni ve kendine özgü bu alana uygulanamayacaktır. O halde, bilişim sistemlerinin günümüz dünyasının vazgeçilmez unsurları olduğu göz önüne alındığında bu sistemler aracılığıyla gerçekleştirilen ihlallerin de gecikmeksizin, hızlı, öngörülü ve değişen çağa uyum sağlayabilecek kapsamda değerlendirilmesi ve düzenlenmesi gerekmektedir.

Bilişim alanının sınırlarının olmaması bu alanda işlenen suçlarla etkili mücadelede sadece ülkelerin ulusal mevzuatlarında yer alan düzenlemelerin yeterli olmayacağı açıktır. Bu bağlamda, suçlarla mücadelede ortak usullerin kararlaştırılıp geliştirilmesi gerektiği gibi maddi ceza hukuku anlamında da aynı veya benzer suç tiplerinin düzenlenmesi, ülke mevzuatında eksiklik bulunan hususlarda diğer ülke örneklerinin göz önünde bulundurulması esasen küresel ortak uygulamaların ve ortak dilin oluşturulması, ulusal yasal mevzuatların birbirlerine uyumlu hale getirilmeleri gerekmektedir. Bilişim suçları alanında en kapsamlı uluslararası belge olan Avrupa Konseyi Siber Suç Sözleşmesi ise bu anlamda en güzel örneği oluşturmaktadır.

Ceza Kanunlarında düzenlenen birçok suç tipinin aksine dinamik bir yapıda olan bilişim suçlarında[4] yapılacak olan yasal düzenlemelerin hızla gelişen günümüz teknolojisi ile ortaya çıkan yeni ihlaller ile mücadelede ihtiyacı karşılayabilmesi adına bu hıza uyumlu ve gelişen yeni durumlara paralel düzenlemeleri ve güncellemeleri gerçekleştirilmesi gerekmektedir. Bu bağlamda, çalışmamızda dar anlamda bilişim suçları olarak kabul ettiğimiz 5237 sayılı Türk Ceza Kanunu' nun (TCK) "Bilişim Alanında Suçlar" bölümünde yer alan suç tipleri çeşitli ve sayıca fazla olan kaynak araştırması ile birlikte doktrinde yer alan fikirler ve Yargıtay kararları ile

4 Olgun Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", *Legal Hukuk Dergisi,* Yıl:2003, Cilt: 1, Sayı: 11, ss. 2750-2758, s. 2758.

zenginleştirilerek maddi ceza hukuku boyutu ile incelenerek yasal düzenlemelerin mevcut durumu günümüz güncel teknolojisinin geldiği noktaya da temas edilerek değerlendirilmek suretiyle suçla mücadelede maddi ceza hukukunda etkili çözüm önerileri getirilmeye çalışılacaktır. Zira, bilişim alanında suçların disiplinler arası bir çalışmayı gerektirdiği değerlendirildiğinden çalışmamız içerisinde ilgili bölümler içerisinde günümüz teknolojileri ve bu alanda yapılan çalışmalara da sıklıkla yer verilmiştir. Diğer taraftan, her ne kadar çalışma konumuzu 5237 sayılı TCK' nın "Bilişim Alanında Suçlar" bölümünde yer alan dar anlamda bilişim suçları oluşturmakta ise de çalışmamız içerisinde bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen geniş anlamda bilişim suçlarına da ilgi bölümlerde konu içerisinde değinilecektir.

Çalışmamız üç ana bölümden oluşmakta olup birinci bölümde "Bilişim Suçlarına İlişkin Temel- Teknik Terim ve Kavramlar ile Genel Bilgiler", ikinci bölümde "Bilişim Suçlarına İlişkin Mukayeseli Hukukta Yer Alan Düzenlemeler ve Yapılan Çalışmalar" ve üçüncü bölümde ise "5237 Sayılı Türk Ceza Kanununda Bilişim Alanında Suçlar" incelenecektir.

Çalışmamızın birinci bölümünde, bilişim alanında gerçekleşen ihlallerin, bu ihlallerin değerlendirilmesinin, esasen suç tiplerinin konusunu oluşturan bilişim sistemlerinin anlaşılması, olaya uygun doğru uygulamanın gerçekleştirilmesi ve bu alana yönelik çözüm önerileri getirilmesinin başlıca yolunun iyi bir ceza hukuku bilgisinin yanında alana özgü teknik bilgiyi de gerektirdiği düşünüldüğünden[5] esasen suç tiplerinin iyi bir şekilde tespiti ve doğru uygulamaların geniş anlamda bilişim suçlarına ilişkin temel ve teknik terim ve kavramların aydınlatılması fikri ile bu kavramlar incelenmiş, günümüzde yaşanan güncel teknolojik gelişmelere de değinilmek suretiyle alana ilişkin terim ve kavramların tanımlanması yolu ile açıklanarak ortak dil kullanımının sağlanması amaçlanmıştır. Bunun yanında, bilişim suçlarına ilişkin genel bilgiler üst başlığı altında ise bilişim suçları kavramsal açıdan değerlendirilerek bilişim suçlarının tanımı, kapsamı, yapısı, özelliklerinin belirlenmesi adına incelemede bulunulmuştur. Ayrıca, ülkeler açısından günümüz dünyasının en önemli konularından birini oluşturan siber güvenlik, kritik altyapı hizmetleri, siber saldırı (ve siber saldırı yöntemleri) ile siber terörizm kavramları incelenmiş, yaşanan güncel olaylara ilişkin örnekler ilgili bölüm içerisine eklenmiş, etkili bir suçla

5 Aynı yönde bkz. Hakan Karakehya, "Türk Ceza Kanununda Bilişim Sistemine Girme Suçu", *Türkiye Barolar Birliği Dergisi*, Yıl: 22, Sayı: 81, Mart-Nisan 2009, ss. 1-24, s. 3.

mücadelenin etkili önlem ve etkili yaptırımlar içeren maddi hukuk normlarının varlığına bağlı olduğu düşüncesi ile de esasen birbirinden ayrılmaz kavramlar olan siber güvenlik ve siber terörizm kavramları incelenerek siber terörizme ilişkin ceza mevzuatımızda yer alan boşluğa ilişkin olarak öneriler getirilmiştir.

Çalışmamızın ikinci bölümünde, bilişim suçlarına ilişkin mukayeseli hukukta yer alan düzenlemeler kapsamında alana ilişkin olarak uluslararası kuruluşların yapmış oldukları güncel çalışmalar ile bilişim suçlarının yabancı ulusal mevzuatlarda var olan düzenlenme şekilleri ayrıntılı bir şekilde incelenerek mevzuatımızda var olan düzenlemelerle karşılaştırılmıştır. Bölüm içerisinde özellikle bu alanda en kapsamlı uluslararası belge niteliği taşıyan Avrupa Konseyi Siber Suç Sözleşmesi' nin maddi ceza hukuku hükümleri incelenerek Ceza Kanunu' muzun uyumluluğu üzerinde incelenerek değerlendirme ve önerilerde bulunulmuştur.

Çalışmamızın üçüncü bölümünde ise çalışmamız içerisinde ayrıntılı olarak açıklanacağı üzere dar anlamda bilişim suçları olarak kabul ettiğimiz ve 5237 sayılı TCK' nın "Topluma Karşı Suçlar" başlıklı üçüncü kısmının "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde düzenlenen "Bilişim sistemine girme" (TCK 243), "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" (TCK 244), "Banka veya kredi kartlarının kötüye kullanılması" (TCK 245) ve "Yasak cihaz veya programlar" başlıklı (TCK 245/A) suç tipleri maddi ceza hukuku hükümleri olarak ve suçun unsurları kapsamında korunan hukuksal değer, maddi unsur, manevi unsur ve hukuka aykırılık başlıkları altında incelenmiştir. Suç tiplerinin düzenlenmiş olduğu maddeler incelenirken konuya ilişkin doktrinde tartışmalı olan hususlara yer verilmiş bunun yanında Yargıtay uygulamaları ve kararları da eklenmiştir. İncelenen suç tipleri arasında benzer suçlarla ilişkisi doktrinde veya uygulamada tartışmalı olan suçlar için bu husus ayrı bir başlık altında incelenerek Yargıtay uygulamaları belirtilmiş ve son olarak konuya ilişkin fikirlerimiz eklenmiştir.

Çalışmamızın sonuç kısmında ise çalışmamız boyunca incelemiş olduğumuz hususlar ışığında 5237 sayılı Türk Ceza Kanunu' nun "Bilişim Alanında Suçlar" bölümünde yer alan suç tipi düzenlemelerine ilişkin tespit, değerlendirme ve önerilerimize yer verilerek çalışmamız sonlandırılmıştır.

BÖLÜM I

BİLİŞİM SUÇLARINA İLİŞKİN TEMEL-TEKNİK TERİM VE KAVRAMLAR İLE GENEL BİLGİLER

1.1. BİLİŞİM SUÇLARINA İLİŞKİN TEMEL TERİM VE KAVRAMLAR

Bilişim suçlarının kendine özgü yapısı ve klasik suç tiplerinden birçok açıdan farklılaşması, bu suç tiplerine Ceza Kanunlarında yer verilmesi yeni ve tanımlanma ihtiyacı bulunan birçok terim ve kavramı ortaya çıkarmıştır. Nitekim, 765 sayılı Türk Ceza Kanunu (TCK) ve şu an yürürlükte bulunan 5237 sayılı Türk Ceza Kanunu (TCK) incelendiğinde bilişim suçlarına ilişkin bazı temel kavramların tanımlanmadığı görülmekte olup çalışma konumuzu oluşturan bilişim suçlarını incelemeye başlamadan önce bazı temel kavramların açıklanmasının, konunun anlaşılması bakımından zorunluluk arz ettiği değerlendirilmektedir.[6] Bu bağlamda,

6 Karakehya, a.g.e., s. 7, 8.
Eker' e göre de: "Ceza hukuku açısından tipiklik unsurunun gereğince tebarüz ettirilmesi ve kanunilik ilkesinin muğlak kavramlarla sakatlanmaması amaçları doğrultusunda iyi ifade edilmiş, sınırları belirlenmiş bir tanım yapmak önemlidir. Bilişim suçları gibi hukukun alanına yeni dahil olmuş, henüz yeterince işlenmemiş/oturmamış teknik bir olgunun da tanımlanıp müesseseleşebilmesi için multi-disipliner bir yaklaşım içerisinde ilgili alanların uzmanlarının ortak bir çalışma yapması olgunun aydınlatılması, sınırlarının anlaşılması ve her şeyden önce tanımlama kriterlerinin belirlenmesi gerekmektedir." 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*, Yıl: 19, Sayı: 62, Ocak-Şubat 2006, ss. 101-131, s. 102.
Yine Dülger de, bilim dilinin kavramsallaştırmanın aracı olduğunu, kavramsallaştırmanın bilimsel çözümleme ve ilerleme yönünde iyi bir dayanak olabilmesi için kavramın kendisine uygun tanımlara dayalı olması gerektiğini, bu bağlamda bilimsel olma iddiasında olan bir çalışmada kullanılan her kavram için açık bir tanım ve belirleme bunun yanında kavramın anlamını tam olarak sınırlama zorunluluğu bulunduğunu belirtmektedir. Ayrıntılı bilgi için bkz. Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 7. bsk., Seçkin Yayınevi, Ankara, 2018, s. 57.
Ancak Dülger şu hususları da belirtmektedir: "…teknoloji alanındaki gelişmelerin çok hızlı olması nedeniyle belli bir teknolojik ortama yönelik yasa ile yapılan tanımlama girişimleri birkaç yıl içinde eskir ve işlevsiz kalır. Bu nedenle Birleşik Krallık hukukunda bu tür aygıtların ya da bileşenlerin kesin bir biçimde tanımlanmasından kaçınılmıştır. Benim de katıldığım ve doğru bulduğum bu bakış açısı ülkemiz mevzuatı açısından da geçerlidir. Hatta ülkemiz bir adım daha öne geçerek "bilişim sistemleri" kavramını kullanarak her yeni gelişmeyi ve aygıtı kapsayabilecek bir düzenleme yapmıştır." Bkz. Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 145.

çalışmamıza klasik suç tiplerinden birçok yönüyle farklılaşan bilişim suçlarını değerlendirebilmek ve anlayabilmek için, bu suç tipinin doğası gereği ilişkili olduğu bir takım temel ve teknik terim ve kavramların açıklanması ile başlamayı uygun bulmaktayız.

1.1.1. Bilişim

Bilişim kavramı, belgeleme tekniğinin ayrı bir disiplin olarak kabulünden sonra doğan ve gelişen bir kavram olup başlarda bilginin saklanması ve erişilmesini sonrasında yaşanan teknolojik gelişmelerle bilginin yönetilmesi ve işlenmesini hedef tutan bir bilim dalı haline gelmiştir.[7] Önceleri dilimize Fransızca "informatique" sözcüğünün çevirisi ile "enformasyon" olarak geçen, kullanılan ve sonradan Türkçeleştirilip türetilen[8], "bilişim" terimi, dilimize Prof. Dr. Aydın Köksal tarafından kazandırılmış ve bu terim ilk kez onun tarafından kullanılmıştır.[9] Dülger' in de belirtmiş olduğu gibi bilgi vermek kökeninden gelen "informatiqe" sözcüğü yerine, anlatmak istediği kavramı en geniş kapsayan terim olması açısından[10] bilgi kökeninden gelen "bilişim" teriminin kabulü ve kullanımının daha uygun ve isabetli olduğu[11] kanaatindeyiz.

5237 sayılı Türk Ceza Kanununda ve gerekçesinde tanımlanmamış olan "bilişim" terimi için aralarında belirgin farklılıklar bulunmamakla birlikte Türk Dil Kurumu sözlüğünde ve hukuk doktrininde yapılmış olan birçok tanım bulunmaktadır.

Türk Dil Kurumunu' nun 1998 tarihli Türkçe Sözlüğü' nde bilişim: *"Teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullanılan ve özellikle elektronik makineler aracılığı ile düzenli bir biçimde işlemeyi ön gören bilim, enformatik"*[12] olarak Türk Dil

7 Berrin Akbulut, *Bilişim Alanında Suçlar*, 2. bsk., Adalet Yayınevi, Ankara, 2017, s. 13.
8 Olgun Değirmenci, *Bilişim Suçları*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2002, s. 4; Caner Yenidünya, Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, Legal Yayıncılık, İstanbul, 2003, s. 27; Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 40.
9 Türksel Kaya Bensghir, "Türkiye' de Yönetim Bilişim Sistemleri Disiplinin Gelişimi Üzerine Düşünceler", *Amme İdaresi Dergisi*, Cilt: 35, Sayı:1, 2002, , ss. 77-103, s. 82; Kurt, a.g.e, s. 23; Yavuz Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* Legal Yayıncılık, İstanbul, 2012, s. 5; Hayati Pallı, *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Kayseri, 2008, s. 34, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020; Ramazan Doğan, *5237 Sayılı Türk Ceza Kanunu' nda Bilişim Suçları,* Adalet Yayınevi, Ankara, 2014, s. 5.
10 Pallı, a.g.e., s. 34
11 Murat Volkan Dülger, *Bilişim Suçları*, Seçkin Yayınevi, Ankara, 2004, s. 45; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 68.
12 *Türk Dil Kurumu Türkçe Sözlük*, Hazırlayanlar: İsmail Parlatır, Nevzat Gözüaydın, Hamza Zülfikar, Belgin Tezcan Aksu, Seyfullah Türkmen, Yaşar Yılmaz, Cilt I, 9. bsk., Sözlük Bilim ve

Kurumu (TDK) Büyük Türkçe Sözlük' te ise: *"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik"*[13] olarak tanımlanmıştır. İngilizce- Türkçe Ansiklopedik Bilişim Sözlüğü' nde de *"informatics: bilişim. İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve rasyonel biçimde işlenmesi bilimi."*[14] olarak tanımlanmıştır. Longman sözlüğünde ise "information science" (bilişim bilimi) *"bilginin toplanması, düzenlenmesi, depolanması, alınması ve (dışa) gönderilmesi bilimi"* olarak tanımlanmıştır.[15]

Aydın ise bilişimi "(informatics/bilgibilimi)"[16] :

> *"... bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler; ve öte yandan da: Bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleri"*[17] şeklinde tanımlamıştır.

Artuk-Gökçen-Yenidünyaya' ya göre bilişim;

> *"insanların teknik, ekonomik, sosyal, kültürel, hukuksal veya benzeri alanlarda sahip oldukları verinin saklanması, saklanan bu verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve yüksek hızlı veri, ses veya görüntü taşıyan iletişim araçları ile aktarılmasıdır."*[18]

Değirmenci bilişimi, *"teknik, ekonomik, sosyal, hukuki alanlardaki verinin, otomatik olarak işlenmesi, saklanması, organize edilmesi, değerlendirilmesi ve aktarılması"*[19]

Uygulama Kolu Yayınları Türkçe Sözlükler Dizisi: 1, Türk Dil Kurumu Yayınları: 549, Ankara, 1998, s. 297.

13 http://tdk.org.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5d9a02a3991702.19216647 ET. 6.10.2019..

14 Bülent Sankur, *İngilizce-Türkçe Ansiklopedik Bilişim Sözlüğü*, 3. bsk., Pusula Yayıncılık, İstanbul, 2008, s. 373.

15 "information science", "the science of collecting, arranging, storing, retrieving (RETRIEVE), and sending out information" bkz. *Longman Dictionary of English Language and Culture*, Second edition, Addison Wesley Longman Limited Edinburgh Gate, England, 1998, s. 676.

16 Emin Doğan Aydın, *Telsim'in katkılarıyla Bilişim ve Telekomünikasyon Terimler Sözlüğü*, Telsim Yayınları-1, İstanbul, Ağustos, 1999, s. 432.

17 Emin Doğan Aydın, *Bilişim Suçları ve Hukukuna Giriş*, 1. bsk., Doruk Yayınları, Ankara, 1992, s. 3.

18 Mehmet Emin Artuk, Ahmet Gökcen ve Ahmet Caner Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, C:V, 2. bsk., Adalet Yayınevi, Ankara, 2014, s. 6902.

19 Değirmenci, "Bilişim Suçları", s. 7.

olarak tanımlamıştır. Özen ve Baştürk ise "*kısaca bilişim, bilginin (verilerin) bilgisayar aracılığıyla elektronik olarak depolanması yanında işlenmesini ve iletilmesini kapsamaktadır."*[20] şeklinde belirtmektedir.

Dülger' e göre ise;

> *"Bilişim, insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişimde kullandığı bilginin özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir."*[21]

Doğan ise bilişimin, bilgi teknolojilerinin tümünü içine alan bir üst kavram olduğunu belirterek kapsayıcı bir tanımlama ile bilişimi:

> *"insanların teknik, ekonomik, toplumsal, hukuk ve benzeri alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin, elektronik makineler aracılığıyla depolanması, işlenmesi, değerlendirilmesi, organize edilmesi, ses, görüntü ve veri taşıyan iletişim hatları ile kullanıcılara ulaştırılması bilimidir."*[22] şeklinde tanımlamıştır.

Erdoğan ise üzerinde hakimiyetimizin olmadığı bir bilim dalını tanımlamamız halinde bazı hususların eksik kalabileceği bu durumun ise bilişim suçlarının uygulanmasında sıkıntı doğurabileceği ve bunun yanında bilişimin sürekli yenilenen ve yaşayan bir bilim dalı olması gerekçesi ve endişesiyle tanımlama yapmak yerine bilişimin temel unsurlarının belirtilmesinin yeterli olduğunu, zira zamanla yetersiz kalabilecek bir tanımlamanın suçta ve cezada kanunilik ilkesinin geçerli olduğu ceza hukuku bakımından telafisi imkansız sonuçlar doğurabileceğini ileri sürmüştür.[23] Bu bağlamda, Erdoğan' a göre bilişimin temel unsurları, verilerin işlenebilmesi, saklanabilmesi ve aktarılabilmesidir.[24]

Son olarak Kurt' a göre bilişim, *"her alandaki üretilmiş bilgileri içeren verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili bilim dalıdır."*[25]

---

20 Muharrem Özen ve İhsan Baştürk, Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku, 1. bsk, Adalet Yayınevi, Ankara, 2011, s. 11.
21 Dülger, *Bilişim Suçları*, s. 47; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 70.
22 Doğan, a.g.e., s. 6.
23 Erdoğan, a.g.e., s. 8; Yavuz Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* Legal Yayıncılık, İstanbul, Şubat 2018, s. 50.
24 A.e., s. 50, 51. Aynı yönde görüş için bkz. Berrin Bozdoğan Akbulut, "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, Milenyum Armağanı, Sayı: 1-2, C: 8, Konya, 2000, s. 546.
25 Kurt, a.g.e., s. 25.

Yargıtay Ceza Genel Kurulu 2007 yılında vermiş olduğu bir kararda, bilişim kavramı için şu açıklamalarda bulunmuştur:

> *"... "bilişim sözcüğü "bilgisayar" kelimesine oranla daha geniş kapsamlıdır. Bilgisayar, (kompütür, elektronik beyin) aritmetik ve mantık işlemi dizileriyle oluşturulmuş programlara göre verileri (bilgileri) otomatik işleme tabi tutan sistemlere verilen ortak isim iken, bilişim (enformatik) ise, bilgisayardan da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesine konu olan akademik ve mesleki disipline verilen addır; yani başka bir deyişle, bilgisayar kullanma ilmidir..."*[26]

Doktrinde yer alan bir başka husus ise bilişim teriminin, bilgisayara göre daha geniş bir alanı kapsayan bir "üst kavram"[27] olduğunu belirten yazarlar[28] bulunmakta ise de kavramsal açıdan bilişimin bir bilim dalı olması bilgisayarın ise bu bilim dalını oluşturan araçlardan bir tanesi olması sebebiyle farklı iki kavramı ifade eden söz konusu iki kelimeyi karşılaştırmanın uygun olmadığı görüşünü savunan Dülger' e[29] katılmaktayız.

1.1.2. Bilgisayar

Teknolojinin hızla ilerlemesi ile bilgisayar özellikleri taşıyan ve bilgisayarların yaptığı işlemleri yapabilen fakat klasik bilgisayar donanım unsurlarını taşımayan bir takım cihazlar hayatımıza girmiş ve günlük yaşantımızın bir parçası haline gelmiş olup işletim sistemine sahip akıllı yeni nesil cep telefonları bunun en güzel örneğini oluşturmaktadır.[30] Bilgisayarların geçirmiş olduğu tarihsel süreç sonrasında günümüzde bilgisayar olarak nitelendirilebilecek çok çeşitli cihazlar bulunmakta ise de bugün itibariyle dijital bilgisayarların temel görev ve işlevleri bakımından genel kabul gören bir takım hususların açıklanmasının, bilgisayarın Türk Ceza Kanunu' nda yer alan bilişim alanında suçların işlenmesinde sıklıkla kullanılan bir araç olması veya suçun konusunu oluşturması bunun yanında esasen akla ilk gelen bir bilişim sistemi

26 Yargıtay Ceza Genel Kurulu 10.06.2007 t., E: 2007/6-136, K: 2007/150, www.kazanci.com›kho2/ibb/giris.html, ET. 13 Temmuz 2020.
27 Taşkın' a göre de, "bilişim bilgi teknolojilerinin tümünü kapsayan bir üst kavram olarak tanımlanabilir" bkz. Şaban Cankat Taşkın, *Bilişim Suçları*, 1. Bs., Beta Yayıncılık, İstanbul, 2008, s. 8.
28 Yenidünya ve Değirmenci, a.g.e., s. 30-31; Eker, a.g.e., s. 104; Erdoğan, *Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 44.
29 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 70
30 A.e., s. 60.

örneği[31] olması açısından büyük önem taşıdığı düşünülmektedir.[32] Dolayısıyla, bu başlık altında bilgisayar öncelikle bir terim sonrasında ise esasen bilişim sisteminin ne olduğunun anlaşılabilmesi adına bir cihaz olarak incelenecek ve faydalı olduğu düşünülen bilgilerden bahsedilecektir.

1.1.2.1. Tanım

Ülkemize 1970' li yıllarda giren ve önceleri bilimsel alan ile iş yaşamında kullanılmaya başlanan[33], ilk başlarda "kompütür", "sayısal makine", "elektronik beyin", "ordinatör" gibi kelimelerle ifade edilen esasen İngilizce'de hesaplamak anlamına gelen "compute" kelimesinin Türkçe karşılığını oluşturan[34] bilgisayar, makinenin gerçek yapılma amacı olan "bilgi işlemek" kökünden türetilerek öz Türkçe olan bu kelime ile adlandırılmıştır.[35] 5237 sayılı Türk Ceza Kanunu' nun 243. m.' sinde yer alan "bilişim sistemi" nin en önemli örneklerinden biri olan bilgisayarın birçok tanımı yapılmıştır.

Türk Dil Kurumu Sözlüğü' nde bilgisayar: *"Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin"*[36] olarak tanımlanmıştır. İngilizce- Türkçe Bilişim Terimleri Sözlüğü' nde ise computer (bilgisayar), *"insan müdahalesi olmaksızın mantıksal ve aritmetik işlemler de dahil geniş kapsamlı hesaplamaları yapabilen işlevsel birim"*[37] olarak tanımlanmıştır.

Başka bir tanımlamada ise bilgisayar şu şekilde ifade edilmiştir:

> *"veri olarak adlandırılan girdilerin bir işlem süzgecinden geçirilerek, sonuçlarını bildiren aygıt; bilgiyi depolayabilen, veri işleyebilen, temel dört işlemin yanı sıra, karar*

---

31 Artuk, Gökçen ve Yenidünya bilgisayarın, bir bilişim sistemi olması dolayısıyla, TCK' nın 243. m.' sinde yer alan suçun konusu içerisinde değerlendirildiğini belirtmektedir. Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6902.

32 Ketizmen de bu konuda, "765 Sayılı TCK'de ve TCK'de "bilişim alanında suçlar" başlığı altında düzenlenen suçlar da genel olarak bilgisayarların kullanımı ile ilgili çeşitli fiillerin esas alınarak cezalandırıldığı suçları içermektedir." fikrini belirtmiştir. Ayrıntılı bilgi için bkz. Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Doktora Tezi, Ankara, 2006, s. 16, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

33 Doğan, a.g.e., s. 8.

34 Pallı, a.g.e., s.4.

35 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 59.

36 *Türk Dil Kurumu Türkçe Sözlük*, 1998, s. 295.

37 *Bilişim Terimleri Sözlüğü İngilizce-Türkçe*, Hazırlayanlar: Ali Arifoğlu, Mehmet Demirer, Gökhan Şengül, Osman Öz, Türk Standartları Enstitüsü, Onur Matbaacılık, İstanbul, Mayıs 2006, s. 40; Yine tanımda "NOT 1: Bir bilgisayar tek bir birimi veya birbirine bağlı birkaç birimi içerebilir. NOT 2: Türkçede, bilgi işlem alanında bilgisayar deyimi genellikle sayısal bilgisayarları ifade eder." hususları eklenmiştir. Bkz A.e.

da verebilen bir araçtır…Bilgisayar aldığı komutlar uyarınca veri işleyerek problem çözen otomatik elektronik aygıtların ortak adıdır."[38]

Bilgisayarın,

"Kullanıcıdan aldığı veri yada bilgilerle kullanıcının isteği doğrultusunda işlem ve karşılaştırmalar yapabilen, veri yada bilgileri hard disk, disket, CD, DVD gibi dış belleklerde istenilen sürece saklayabilen, istenilen şekilde yazılı, ses, görüntü olarak çıktı verebilen elektronik makinelerdir"[39] şeklinde tanımı da bulunmaktadır.

Diğerlerine nazaran daha genel bir tanımlamada ise bilgisayar, *"kullanıcıdan giriş birimleriyle aldığı komutları işleyerek çıkış birimleri aracılığı ile kullanıcısına sunan elektronik aygıtların genel adıdır."*[40] şeklinde ifade edilmiştir.

Hukuk doktrininde yer alan bilgisayar tanımlarından bir tanesinde, Yazıcıoğlu, Türkçe' de "elektronik beyin" veya "kompütür" yahut "ordinatör" veyahut "bilgileri otomatik işleme tâbi tutmuş sistem" olarak da adlandırılan "bilgisayar" ın, önceden saptanan işlemleri, belli bir sıraya göre -dört-beş adet temel işlem dahilinde (toplama, çıkarma, çarpma, bölme, üs alma ve mantıksal karşılaştırma)- yapan ve dış ortamdan aldığı verileri işleyen elektronik özellikli bir araç[41] olarak tanımlanmıştır. Aydın ise:

"computer: Bilgisayar Merkez işlem birimi (CPU), ana bellek ve güç kaynağı ihtiva eden bir ana kabin ile, buna bağlı gidiş/ çıkış (I/O), veri saklama gibi çevre birimleri ve birimlerden oluşan genel amaçlı bir bilgi işlem sistemi. Geleneksel bir bilgisayar sisteminde sadece merkez işlem birimi en az bir ve hatta çoğu zaman birden fazla kabin gerektirir."[42] şeklinde açıklama yapmıştır.

Kurt ise ayrıntılı ve kapsamlı bir bilgisayar tanımı yaparak

"programlara ve verilen komutlara göre işlem yapan otomatik olarak çalışan, sıralı işlem yapan, verileri depolama, işleme tabi tutma, tasnif ve terkip etme, iletme özelliklerine sahip olan, elektronik ya da manyetik akımlarla çalışan, mantıklı sonuçlar üreten, programlanabilen, genel amaçlı kullanılabilme özelliklerine sahip elektronik cihazlar"[43] olarak tanımlamıştır.

---

38 Mustafa Uludoğan, *Eğitimde Bilgisayar Okur Yazarlığı Bilgisayara Giriş Ders Kitabı*, Atlas Yayın Dağıtım, İstanbul, Ocak, 2002, s. 1.

39 "Bilgisayara Giriş Ders Notları", s. 1, http://web.iku.edu.tr/~tkaynas/bgdn2.pdf, ET. 12 Ekim 2019.

40 Levent Emmungil, *Bilgisayar Donanımı*, Ankara, 2010, E-Kitap, s. 2, http://it.famergroup.com/bilgisayardonanim.pdf, ET. 13 Ekim 2019.

41 Recep Yılmaz Yazıcıoğlu, "Şifreli Yayınların Bilişim Suçları Karşısındaki Konumu", *Yargıtay Dergisi*, Cilt: 25, Sayı: 1-2, Ocak-Nisan 1999, s. 58.

42 Aydın, *Telsim'in katkılarıyla Bilişim ve Telekomünikasyon Terimler Sözlüğü*, s. 162.

43 Kurt, a.g.e., s. 31.

Akbulut ise bilgisayarı, *"insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler"*[44] olarak tanımlamıştır. Dülger' e göre ise:

> *"Bilgisayar, bir giriş- çıkış aygıtı ve bir belleği bulunan, her türlü simgeleştirilmiş işlemi yapabilen ve bu işlemleri belleğine kaydedilmiş yazılımlarla gerçekleştirilen bir ana işlemciye sahip, veriler üzerinde dönüştürme işlemi yapan işletim yazılımı bulunan, bilgileri belirli bir düzende saklayan, üzerine farklı yazılımlar yüklenilebilip aynı yöntemle çıkartılabilen, veri iletişimini sağlayan, salt bir konuya özgülenmemiş, her türlü işlemi yapabilmek için genel amaçlı olarak üretilmiş makinelerdir."*[45]

Bir başka tanımlamaya göre ise bilgisayar: *"belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen masaüstü, dizüstü bilgisayarlar, cep telefonu ve benzeri tüm elektronik araçları ifade eder."*[46]

Görüldüğü üzere bilgisayarın birçok tanımı yapılmışsa da her tanım gelişen dünya, gelişen teknoloji karşısında yetersiz kalabilmektedir. Nitekim, belirtilmiş olan tanımlara uymayan ancak bilgisayarın işlevlerini yerine getirebilen ve hatta bir bilgisayarın özelliklerini taşıyan işletim sistemine sahip akıllı cep telefonları, kişi ya da araçları elektronik olarak tanıyan güvenlik araçları,[47] akıllı saatler, IoT (internet of

44 Akbulut, *Bilişim Alanında Suçlar*, s. 10,11; Bozdoğan Akbulut, "Bilişim Suçları", s. 546.
45 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 66.
46 Murat Volkan Dülger ve Gözde Modoğlu, Bilişim Suçları, *Soruşturma ve Kovuşturma Yöntemleri İle İnternet İletişim Hukuku (Uygulama Rehberi),* Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği/Avrupa Konseyi Ortak Programı, y.y., t.y., s. 25; Murat Volkan Dülger ve Gözde Modoğlu, *Bilişim Suçları Eğitim Modülü*, Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği/Avrupa Konseyi Ortak Programı, y.y., t.y., s. 55.
47 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 70.

things veya nesnelerin interneti[48]) teknolojisine sahip akıllı cihazlar[49], yapay zeka[50] teknolojisine sahip ürünler, otonom araçlar gibi birçok araç ve cihazın ortaya çıkması

48 "Nesnelerin İnterneti, birbirleriyle belirli bir protokol üzerinden haberleşen, bilgi paylaşan, kontrol edilebilen cihaz topluluklarından oluşan ağa verilen isimdir. Bu ağ, günümüzde her alana uygulanabilen bir yapı haline gelmiş olup, sanayiden tarıma enerji sistemlerinden ev otomasyonuna, lojistikten sürüş konforuna, sağlıktan otomotive, savunma sektöründen askeri sistemlere pek çok alanda karşımıza çıkmaktadır." Bkz. Şeref Sağıroğlu, "Siber Güvenlik ve Ötesi", *Siber Güvenlik ve Savunma : Problemler ve Çözümler*, Ed.: Şeref Sağıroğlu, Mustafa Şenol, BGD Siber Güvenlik ve Savunma Kitap Serisi 2, 1. bs., Grafiker Yayınları, Ankara, 2019, ss. 25-58, s. 48.

49 " "Nesnelerin Interneti (IoT: Internet of Things)" olarak adlandırılan yeni teknolojik kavram akıllı cihazların, birbirlerini algılayan ve iletişime geçebilen nesneler aracılığıyla akıllı bağlantısı şeklinde tanımlanmaktadır. Bu teknoloji ile çok sayıda, küçük boyutlu, kablosuz teknoloji kullanabilen algılayıcı (sensor) cihazlar ile yaşadığımız çevredeki (ev, okul, işyeri, fabrika, şehir vb.) hemen hemen bütün olayları izlemek ve bilgi toplamak mümkündür." Bkz. Tuncay Ercan, Mahir Kutay, "Endüstride Nesnelerin Interneti (IoT) Uygulamaları", *Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi,* 2016, ss. 509-607, s. 509, https://fenbildergi.aku.edu.tr/wp-content/uploads/2016/12/035102-599-607.pdf, ET. 19 Ekim 2019.

"Hem internet ağıyla hem de birbiriyle bağlantılı cihazlar, hackerler için yeni saldırı yüzeyleri oluşturuyor. Yapılan hataların başında güvenliğinden emin olunmayan ortak Wi-Fi ağlarına bağlanmak geliyor. Araştırmaya göre, hackerlerin restoran, otel veya havaalanları gibi mekanlardaki şifresiz Wi-Fi ağlarına kolayca bağlanabileceğini dikkate alınmıyor." Bkz. CYBERMAG, "IOT CİHAZLAR İÇİN YETERLİ GÜVENLİK ÖNLEMİ ALINMIYOR!", 16.11.2018, https://www.cybermagonline.com/iot-cihazlar-icin-yeterli-guvenlik-onlemi-alinmiyor, ET. 22 Ekim 2019.

"Kullanıcılar için en uygun havayolu biletlerini bulabilen, aktarma ve bekleme sürelerini hesaplayabilen, rezervasyon yapabilen, banka hesap bakiyelerini kontrol ve teyit eden, gidilecek lokasyondaki hava durumu konusunda bilgiyi paylaşabilen, kullanılan ilaçların alınabilmesi için zaman aralıklarını hatırlatabilen, yapılacak satın alımlarda kredi limitlerinin yeterliliği konusunda bilgi veren, sorulan soruları anında yanıtlayabilen ve hatta kullanıcıların yerine düşünebilen IoT cihazların kullanımı giderek artıyor…

IoT cihazlar arasında olan akıllı radyatör, soğutucu, bulaşık ve çamaşır yıkama makineleri, aydınlatma, güvenlik kamerası, alarm sensörleri ve TV'lerin üretimine başlayan yüzlerce farklı üretici bulunuyor. Ayrıca, IoT cihazlar ile sosyal medya platformlarının yönetilmesi üzerine entegrasyon çalışmaları da yapılıyor. Bu bağlamda evde hasta bakım ve çocuk gözetim sistemleri ile entegrasyon, kişisel asistanlığın bir diğer gündem maddesini oluşturuyor. Dolayısıyla bütün bu sistemi, mobil teknolojiler ve yapay zeka uygulamaları ile sağlamlaştıran bir otomasyon teknolojisi olarak tanımlamak yanlış olmaz." Bkz. CYBERMAG, "IOT CİHAZLAR KİŞİSEL VERİ GÜVENLİĞİNİ TEHDİT EDİYOR", 28.09.2018, https://www.cybermagonline.com/iot-cihazlar-kisisel-veri-guvenligini-tehdit-ediyor, ET. 23 Ekim 2019.

50 "Yapay Zeka bilgi edinme, algılama, görme, düşünme ve karar verme gibi insan zekasına özgü kapasitelerle donatılmış bilgisayar olarak da tanımlanabilir.

Bu tür sistemlere matematiksel problemleri çözebilen bilgisayar sistemleri, doğal dili anlayabilen sistemler, bir okulun haftalık ders programını hazırlayabilen bilgisayar sistemi, bir şirketin personel planlamasını yapabilen bir bilgisayar sistemi örnek olarak verilebilir…" bkz. Funda Dağ, "Yapay Zekâ: Temel Kavramlar", *Türkiye Bilişim Ansiklopedisi*, ss.935-939, s. 936.

"Yapay zeka, bilgisayarın veya bilgisayar kontrolündeki bir robotun çeşitli faaliyetleri zeki canlılara benzer şekilde yerine getirme kabiliyetidir… Yapay zeka çalışmaları genellikle insanın düşünme yöntemlerini analiz ederek, bunların benzeri yapay yönergeleri geliştirmesine yöneliktir. Yani bilgisayarın, insanlar tarafından gerçekleştirilen görevleri yerine getirmesini sağlar. Başka bir deyişle, Yapay zeka bilgisayarın insanlar gibi düşünmesini sağlar. Makinelerin karmaşık sorunları insana benzer şekilde çözmesine yardımcı olur. Zeka ve akıl gerektiren sorunlar artık bilgisayar yardımıyla etkili bir şekilde çözülebilir." Bkz. HÜRRİYET, "Yapay zeka nedir? Yapay zeka ne demek?" Hürriyetcom.tr, 6.07.2018, http://www.hurriyet.com.tr/teknoloji/yapay-zeka-nedir-yapay-zeka-ne-demek-40888243, ET., 18 Ekim 2019.

"Günümüzde pek çok sektörde kullanılmaya başlanana yapay zekâ ve makine öğreniminin öne çıkan özellikleri arasında, verileri programatik araçlardan ve insandan çok daha hızlı analiz edebilmesi ve verilerin nasıl işleneceğini kendi kendine öğrenebiliyor olması bulunuyor." Bkz. SİBERBÜLTEN,

karşısında doktrinde de bilgisayar tanımının kabulü gerektiği yönünde belirtilen görüşlere[51] katılmakla birlikte bilişim alanında suçların işlenmesinde en önemli ve yaygın araç[52] veya suçun konusunu oluşturan bilgisayarlar için yapılacak

"Yapay Zekâ, Veri Güvenliği ve GDPR", 2.04.2018, https://siberbulten.com/makale-analiz/yapay-zeka-veri-guvenligi-ve-gdpr/, ET. 21 Ekim 2019.

"Forcepoint, yetenekleri ve kullanım alanı artan yapay zekayı 2019 siber güvenlik tehditleri raporunda ele aldı. Önümüzdeki yıl, yapay zeka odaklı siber saldırıların ciddi zararları gündeme gelebilir.

Siber güvenlik konusunda dünyanın önde gelen şirketlerinden Forcepoint, 2019 yılına ait siber tehditlere dair öngörülerini özel bir raporla açıkladı. Şirket, yapay zekanın hızla artan kullanımının yaratabileceği risklere dikkat çekerken yapay zeka temelli siber saldırılara yönelik uyarılarda bulundu…

Raporun, özellikle kritik altyapı ve ulusal istihbarata yönelik tehditlere vurgu yaptığını kaydeden Turan, yapay zekaya kontrolsüz bir geçişin oluşturabileceği risklere dikkat çekti. İşletmeler ve hükümetlerin bağlantılı sistemlerin sadece kritik verileri ve fikri mülkiyeti değil, aynı zamanda fiziksel güvenliği de riske attığı bir dünyayla karşı karşıya olduğumuzu kaydeden Turan, raporun bu alanlara odaklandığını ifade ediyor." bkz. CYBERMAG, "2019'un Siber Tehditleri İşletmeleri Yeni Önlemler Almaya Zorlayacak", 13.11.2018, https://www.cybermagonline.com/2019un-siber-tehditleri-isletmeleri-yeni-onlemler-almaya-zorlayacak, ET. 23 Ekim 2019.

51 Doğan' a göre: "Bilgisayarların işlevleri konusunda birçok tanım yapılsa da hızla gelişen teknoloji ve bu süreçte bilgisayarların işlevlerinin artması nedeniyle kısa bir süre sonra tanımın yetersiz kalması kaçınılmaz olmaktadır. Ancak ceza hukuku bakımından tanımın yapılmasında zorunluluk vardır. Suçta kanunilik ve tipiklik ilkesi uyarınca bir fiilin suç sayılması için maddi unsurlarının kanunda tanımlanmış olması gerekir. Maddi ceza hukukunda kıyas yapmanın mümkün olmadığı dikkate alındığında suç sayılan fiil için cezasızlık sonucunu doğuracak kanuni boşlukların bırakılmaması gerekir. Bunun için gelişen teknoloji ile uyumlu yasaların yapılması, hukuk kurallarının teknolojik gelişmelerin gerisinde kalmamaları yönünden de zorunludur." Bkz. Doğan, a.g.e., s. 8-9.

Kurt da: "Uluslararası hukuk ve doktrinde bilgisayarın tarifini yapmanın doğru olmadığı vurgulansa ve hızla gelişen teknolojik gelişmeler karşısında riski büyük olsa da işlevsel bir tanımlama yapmak mümkündür. 1991 yılından beri yürürlükte olan "bilgileri otomatik işleme tabi tutan sistem" ve 1 Haziran 2005 tarihinde yürürlüğe giren "bilişim sistemi" kavramları içinde yer alıp almadığını tespit bakımından da tanımlama yapmak zaruridir." Bkz. Kurt, a.g.e., s.28.

Özen, Baştürk' e göre de: "bilgisayarların 'veri depolama' ve 'işleme' olarak iki temel fonksiyonu bulunmaktadır. Teknolojideki gelişmeler karşısında, hukukta bilgisayar kavramının Sözleşme' dekine benzer şekilde geniş anlamını benimseyerek, belirtilen fonksiyonları barındıran tüm araçları bilgisayar olarak kabul etmekte yararlı olacaktır." Bkz. Özen ve Baştürk, a.g.e., s.11.

Pallı' ya göre ise: "… Yani bilgisayarı ne şekilde tanımlarsak tanımlayalım veya hangi yöntemi uygularsak uygulayalım, gelecekte bir yerde kavram bazında çıkmaza girileceği aşikâr olacaktır. Bilgisayar ve başka aygıtlar vasıtasıyla işlenecek suçlarla ilgili yargılamalarda suçta kanunilik ve tipiklik ilkesi uyarınca suçun unsurları belirlenirken en başta kavram boyutuyla değerlendirme yapılacak olması, kavramlar arasındaki sınırların belirlenmesini zorunlu kılmakta, maddi ceza hukukunda kıyas yapmanın mümkün olmaması nedeniyle teknolojik gelişime uygun yeni yasalar yapmanın zorunlu olduğu sonucuna varılmaktadır." Bkz. Pallı, a.g.e., s. 7.

52 "Durmaksızın gelişen bulut, mobil ve IoT trendleri ile birlikte ağ tehditleri de büyüyor ve daha sofistike hale geliyor. Gelişmiş Kalıcı Tehditler (APT'ler) daha hızlı yayılıyor. Günümüzde, ağ saldırılarının yüzde 70 kadarında şifreleme kullanıldığı için, paket içeriği üzerinde geleneksel tehdit algılama giderek zorlaşıyor ve bu da yüksek oranda hatalı bir kurumsal ağ tehdidi analizi ve gecikmeli yanıt oranı ile sonuçlanıyor." bkz. CYBERMAG, "HUAWEI'den Yapay Zekalı Firewall Güvenlik Duvarı", 11.11.2018, https://www.cybermagonline.com/huaweiden-yapay-zekali-firewall-guvenlik-duvari, ET. 24 Ekim 2019.

"● Siber güvenlik uzmanları, ortaya çıkan bu 7 teknolojinin bilgisayar korsanlarının işlerini kolaylaştırdığı konusunda uyarıyor.

● Yapay zekâ, bilgisayar ve kablosuz ağlardaki gelişmelerle teknolojiyi daha hızlı ve güvenli hale getiriyor. Ancak yeni siber güvenlik tehditlerini de beraberinde getiriyor.

● Kötü niyetli kişiler, insanların yeni teknolojileri nasıl kullandığını anlayıp, daha yeni sistemlerin güvenliğinde keşfedilmemiş olan arka kapıları kullanıyor.

tanımlamalarda kısıtlayıcı, daraltıcı tanım ve ifadelerden kaçınmamız gerektiğini de belirtmek isteriz.[53] Zira, bilişim suçlarının çok geniş, sürekli yenilenen ve yeni suç işleme modellerinin ortaya çıktığı bir alan olması neticesinde bilgisayarlar bilişim alanında suçların işlenmesinde en önemli ve yaygın araç veya suçun konusunu oluştursa da 5237 sayılı TCK' da da kapsayıcı olması açısından "bilişim sistemi"

İnsanların ses ve videoları gerçek görünecek şekilde manipüle etmelerini sağlayan 'Deepfake' teknolojisi, son yılların belki de en çok kullanılan yöntemlerinden biri.
Deepfake giderek daha sofistike hale geliyor. Siber güvenlik uzmanları, bilgisayar korsanlarının kimlik avı dolandırıcılığı için teknolojiyi kullanabileceğinden endişe ediyor. Burada bilgisayar korsanları mağdurların özel bilgilerini teslim etmelerini sağlamak için başka biri olarak poz veriyorlar.
Bazı şirketler, deepfake videoları tespit etmek için yapay zekâ güdümlü yazılımlar üzerinde çalışıyor…
Google, geçen ay 'kuantum üstünlüğünü' ilan edecek şekilde gelişmiş şekilde çalışan bir kuantum bilgisayar inşa ettiğini açıkladı. Bu duyuru aslında bir dönüm noktasıydı.
Kuantum bilgisayarlar bu amaçla henüz bilgisayar korsanları tarafından kullanılmamasına rağmen uzmanlar teknolojinin gelecek yıllarda korsanların eline geçebileceğinden endişe duyuyor. Banka gibi kuruluşların yıllarca korudukları şifreleri veri setlerini tehdit ediyor…
5G, daha fazla cihazı desteklemek için hem bant genişliği hem de daha hızlı kablosuz internet vadediyor. Yeni nesil kablosuz ağ olarak ortaya çıkan bu teknoloji, korsanların ağı kullanan sistemleri hedef alma konusunda yeni yıllar açabilir.
Yani en azından güvenlik uzmanlarının görüşü bu yönde. Güvenlik Bulvarı'na göre hızın artması, 5G cihazlarının DDoS saldırına karşı daha hassas hale getirebilir ve bu da kurbanların sunucularını trafiğe boğmak anlamına gelebilir.
Nesnelerin interneti, internete bağlı cihazlar ve bu cihazların birbirleriyle iletişim kurmasını sağlayan ağlara verilen genel bir isim.
Ancak bu teknoloji daha yaygın hale geldikçe, bilgisayar korsanlarının nesnelerin interneti ağlarında güvenlik açıklarını artırabilir. Bunlar şirketlerin operasyonlarını tehlikeye atmak için kullanılabilir...
Yapay zekâ karmaşıklık ve çok yönlülükle ileriye dönük adımlar attığından korsanlar zaten bunu siber güvenlik önlemleri almak için kullanıyor. Bilgisayar korsanları, zayıf noktaları bulmak için ağları hızlıca taramak amaçlı yapay zekâya odaklanan yazılımlar geliştiriyor.
Siber güvenlik şirketi Darktrace CEO'su Nicole Egan, Wall Street Journal'a verdiği demeçte, 'Saldırganların, makine öğrenmesini ve yapay zekâyı saldırının bir parçası olarak kullandıkları zaman olacağını düşünüyoruz' dedi…
Giderek artan sayıda veri ihlali, 'tedarik zinciri' saldırılarının bir sonucu olarak ortaya çıktı. Bu eğilim, bilgisayar korsanlarının hedefleyebileceği potansiyel mağdurlar yelpazesini genişleten üçüncü şahıslara hizmet veren artan sayıda şirket ve kuruluşun sonucu olarak görülüyor…" bkz. Yunus Emre Şahin, "Siber güvenlik uzmanları bu 7 teknolojinin bilgisayar korsanlarının işlerini kolaylaştırdığını söylüyor", 2.10.2019, https://www.gzt.com/bilim-teknoloji/siber-guvenlik-uzmanlari-bu-7-teknolojinin-bilgisayar-korsanlarinin-islerini-kolaylastirdigini-soyluyor-3512558, ET. 24 Ekim 2019.

53 Benzer yönde fikirde olan Artuk, Gökcen, Yenidünya' ya göre: "… birçok isimle adlandırılan bilgisayarın, tüm fonksiyonlarını belirten bir tanımının yapılması zor olduğu gibi, günümüz teknolojisinin hızlı gelişimi karşısında yapılacak bir tarifin zamanla yetersiz kalacağı da söylenebilir… Bu itibarla bilgisayar kavramını tanımlarken, bu aygıtın çalışma prensibi ve fonksiyonları önem kazanmaktadır." Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s.6900-6901.
Yine Erdoğan' a göre de: "bilgisayar teknolojisinin şu ana kadar hiçbir araçta olmadığı kadar hızlı yenilenen bir teknoloji olması nedeniyle, tüm özelliklerini kapsayan bir tanım yapmak mümkün değildir. Bu nedenle biz, bilişim suçları bakımından bilgisayar olarak kabul edilebilecek cihazların veri alma, saklama ve gönderme özellikleri taşıyan cihazlar olduğunu belirtmekle yetiniyoruz.": bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 24.

terimi kullanılmıştır.[54] Dolayısıyla, bu başlık içerisinde bilgisayar, genel kabul gören unsurları ve çalışma mantığı ("bilişim sistemi" nin unsurları ve çalışma mantığı ile aynı temele dayanması bakımından) açıklanmak suretiyle incelenecektir.

1.1.2.2. Unsurlar

Bilgisayarlar fiziki parçalardan oluşan hardware (donanım), elle tutulamayan, gözle görülemeyen software (yazılım) unsurlarından oluşmaktadır.[55] Bir başka deyişle, bilgisayarın elektronik kısmına donanım (hardware), program kısmına yazılım (software) denilmektedir.[56] Bir bilgisayarın çalışabilmesi için somut ve fiziki parçalarının yanında (donanım) soyut bileşenlerinin de (yazılım) bulunması gerekmektedir. Zira, bir bilgisayarları kullanabilmek için tek başına donanım unsuru veya unsurları yeterli olmamakta bir bilgisayarın istenilen bir işlemi gerçekleştirebilmesi için ona, yazılım bileşeninin gerçekleştirebildiği "onun anlayacağı dilde" komutlar verilmesi gerekmektedir.[57]

1.1.2.2.1. Donanım

Bilgisayarın "elektronik ve mekanik bölümü"[58] olarak da ifade edilen hardware (donanım) unsuru, esasen bilgisayarın üzerinde bulunan tüm fiziksel elektronik birimlerine verilen isimdir.[59] Başka bir ifade ile kişisel bir bilgisayarın, işlev ve fonksiyonlarını yerine getirebilmesi için gerekli olan her türlü elektronik ve elektromanyetik parçaların bütünü donanım unsurunu ifade etmektedir.[60] Her ne kadar

54 A.e., s. 71.
"Kablosuz taşınabilir cihazların gelişmesi (örneğin, akıllı cep telefonları), birçok bireyin bilgisayar hakkındaki tanımlamasıyla uyuşmaz. Televizyonlardan çamaşır makinelerine kadar genel olarak "Nesnelerin İnterneti" (Internet of Things / IoT) olarak adlandırılan nesnelerin içine yarı iletken ciplerin entegre edilmesi süreci, bunların birer bilgisayar olarak kabul edilmesi ve bu nesnelerin yetkisiz kullanılması halinde cezalandırmanın sınırlarının genişletilmesine yol açmıştır. Geleceğin taşınabilir cihazlarına internet iletişimi sağlayacak sistemlerin gömülmesi, bir yandan uzaktan kontrol edilebilir nesnelerin işlevselliğinin artırılması olasılığının habercisi olurken, diğer yandan yeni tür suç aktivitelerinin de ortaya çıkmasına yol açacaktır." Bkz. Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 145.
55 Akbulut, *Bilişim Alanında Suçlar*, s. 11.
56 Dülger ve Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet İletişim Hukuku (Uygulama Rehberi)*, s. 25; Dülger, Modoğlu, *Bilişim Suçları Eğitim Modülü*, s. 55.
57 "Bilgisayara Giriş Ders Notları", s. 4.
58"Bilgisayara Giriş", s. 1, http://kisi.deu.edu.tr/huseyin.avunduk/bilgisayara_giris.pdf, ET. 12 Ekim 2019.
59 Ömer Gözü ve Selçuk Han Aydın, *Temel Bilgisayar Kullanımı*, Ed: Hasan Nadir Derin, Feride Erdal, Sürüm 3, Orta Doğu Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı, Aralık 2009, s. 6, http://file.cc.metu.edu.tr/ccweb/bidb_ccusg/TBK2009pub.pdf, ET. 12 Ekim 2019.
60 "Bilgisayara Giriş Ders Notları", s. 5.

gelişen teknoloji ile birlikte yeni birçok donanım aygıtı ortaya çıkabilmekte ve donanımın ikili veya dörtlü sınıflandırmaları bulunmakta ise de bir bilgisayarın donanım unsurunun, giriş birimleri, sistem birimleri, çıkış birimleri ve saklama birimleri olarak dört şekilde sınıflandırmanın bilgisayar ve işlevlerini anlama açısından daha uygun olduğu kanaatindeyiz.

1.1.2.2.1.1. Giriş Birimleri

Bilgisayara "bilgi göndermek"[61] veya veri girmek için kullanılan aygıtlardır. Klavye (keyboard), fare (mouse), digital kamera, tarayıcılar (scanner), CR-ROM sürücü, DVD ROM sürücü, televizyon ve radyo kartı ve benzeri birçok aygıt[62] bu grup içinde yer almakta olup teknolojik gelişmelerle her geçen gün bu grupta yeni donanımlar ortaya çıkarmaktadır.[63] Örnek vermek gerekir ise artık dijital fotoğraf makineleri ve telefonlarımız da girdi aygıtları (giriş birimleri) arasında değerlendirilmektedir. [64]

1.1.2.2.1.2. Sistem Birimleri

"Bilgi işlem elemanları" olarak da ifade edilebilen söz konusu donanım birimi, bilgisayarın temel işlevlerini gerçekleştiren ve çevre birimlerle ilişkilerini düzenleyen donanımlardan oluşmaktadır.[65]

1.1.2.2.1.2.1. Ana Kart

Bilgisayara takılan bütün donanımlar arasındaki bağlantıyı sağlayan[66], diğer tüm kartları üzerinde barındırabilen ve yönetimini sağlayan temel donanım parçasıdır.[67] Başka bir anlatımla, tüm verilerin iletim işlemi üzerinden yapıldığı, birimler arasında iletişim ve kontrol birimi olup üzerinde barındırdığı BIOS (Basic Input/Output System) ile bilgisayarın açılışındaki kontrol işlemleri ve işletim sisteminin yüklenmesinin hazırlığı anakart biriminde yapılmaktadır.[68] Temel olarak

61 Esen Yıldırım, "C++ Programlama, MKÜ - Bilgisayar Mühendisliği Algoritmalar ve Programlama Ders Notları", s. 3, http://hpss.endustri.cu.edu.tr/ders/ENS255/383_dosya_1341385774.pdf, ET. 12 Ekim 2019.
62Ayrıntılı bilgi için bkz. "Bilgisayara Giriş Ders Notları", s. 5-9; Gözü ve Aydın, a.g.e., s. 6, 7.
63 A.e., s. 5.
64 A.e.
65 "Bilgisayara Giriş Ders Notları", s. 9.
66 A.e.
67 "Bilgisayara Giriş", s. 3.
68 Emmungil, a.g.e., s. 11.

bütün bileşenler (harici veya dahili olarak) anakarta bağlandığı için bunlar arasındaki veri yolları ile işlemci ve bellek gibi çeşitli birimlerin ihtiyaç duyduğu enerjinin kontrolü anakart tarafından sağlanmakta olup anakart üzerindeki tüm bileşenlerin iletişimi ise anakartın üzerindeki yongalar[69] aracılığı ile sağlanmaktadır.[70]

1.1.2.2.1.2.2. Merkezi İşlem Birimi (CPU- Central Processing Unit)

Microişlemci veya işlemci olarak da adlandırılan merkezi işlem birimi, bilgisayarın tüm devrelerinin bağlı olduğu, tüm işlemleri belli bir düzen içinde yapan, denetleyen, bu şekilde anlamlı sonuçlar üreten ve bilgisayarı çalıştıran ana kartın üzerinde yer alan tümleşik bir devredir.[71] Bilgisayardaki komutları kontrol eden ve işletmekten sorumlu olan bu ünite[72], bilgisayarın tüm işlemlerini denetleyen, kendisine verilen komut serilerine bağlı olarak istenilen işlemin gerçekleştirildiği, sonrasında ise sonucu emredilen yere gönderen bilgisayarın yegane parçasıdır.[73] Diğer bir anlatımla, işlemci, bilgisayarın birimlerinin çalışmasını ve bu birimler arasındaki veri (data) akışını kontrol eden, veri işleme (verileri değerlendirip yeni veriler üretme) görevlerini yerine getiren elektronik aygıt[74] olarak ifade edilmektedir. Genellikle çip olarak adlandırılan, bilgisayarın içine yerleştirilmiş bir mikroişlemci olan merkezi işlem birimi, bilgisayardaki tüm aritmetik ve mantıksal işlevleri yerine getirmekte, bilgisayarın işletimini kontrol etmekte olup bu aygıtın bizatihi kendisi birçok vakıada delil olabilmektedir.[75]

CPU, toplama, çıkarma, çarpma, bölme gibi aritmetiksel işlemler, karşılaştırma büyüklük, küçüklük, eşitlik tespiti gibi mantıksal işlemleri gerçekleştirmesinin yanında aynı zamanda bilgisayar birimlerin çalışması ve bu birimler arasındaki veri akışını da kontrol etmekte olup bir programdaki talimatları alıp program tarafından

69 "Daha önceden kuzey köprüsü ve güney köprüsü olarak adlandırılan iki farklı yonga seti, gelişen teknoloji ile birleştirilmiş ve güney köprüsü kaldırılarak anakartın üzerinde PCH (Platform Controller Hub) tek bir yonga seti oluşturulmuştur." Bkz. Mehmet Can Karagöz, *Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244),* Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Yüksek Lisans Tezi, Antalya, 2019, s. 31, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.
70 A.e.
71 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 62, 63.
72 Mesut Orta, *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi ve Sunulması (Adli Bilişim),* Yetkin Yayınları, Ankara, 2015, s. 33.
73 Uludoğan, a.g.e., s. 7.
74 Arda Serpen, "Temel Bilişim Teknolojilerine Giriş", Hacettepe Üniversitesi, Powerpoint Sunum, 7.10.2008, s. 18, http://yunus.hacettepe.edu.tr/~denizbas/gmu126/DONANIM.pdf, ET. 12 Ekim 2019.
75 Leyla Keser Berber, *Adli Bilişim (Computer Forensic),* Yetkin Yayınları, Ankara, 2004, s. 54, 55.

istenen işlemleri gerçekleştiren araçtır.[76] Örneğin; harddisk' te yazılı bulunan bir kişinin adresini, buradan daha hızlı olan RAM' e alıp üzerinde gerekli düzenlemeleri yaptıktan sonra kullanıcıya sonucu, yazıcıdan veya ekrandan bir adres etiketi olarak çıkartmak diğer bir deyişle bilgisayarın parçaları arasındaki bilgi transferi, ara işlemler ve sonucun ekran, yazıcı gibi son parçaya iletilmesi işlemleri CPU tarafından gerçekleştirilmektedir.[77]

1.1.2.2.1.2.3. Bellek

"Bellek, bilgisayarda bir programla ilgili bütün komut ve verilerin işlem görmek üzere depo edildiği, değişik işlemler sırasında oluşan ara ve sonuç bilgilerinin saklandığı kayıt ortamlarıdır."[78] Başka bir ifade ile, bilgisayarda çeşitli programların çalıştırıldığı, geçici veya kalıcı bilgilerin (veya verilerin) yer saklanabildiği hafıza alanlarına da bellek adı verilmektedir.[79]

1.1.2.2.1.2.3.1. Rastgele Erişilebilen Bellek (RAM- Random Access Memory)

RAM bilgisayarda çalışan her programın CPU'da çalışmak için bekletildiği ve o ana kadar çalışması sonucunda biriken verilerinin saklandığı hafıza ünitesidir.[80] Başka bir anlatımla "bilgisayara girilen verilerin üzerine yazıldığı ve saklandığı, üzerindeki verilerin silinebildiği ya da değiştirilebildiği, bilgisayarın üzerinde işlem yaptığı bellektir."[81] RAM, genellikle bilgisayardaki ana hafıza ya da birincil depo olarak kullanılmakta olup içerisine bilgi yazılması ve istenildiği zaman bu bilgilere ulaşılması için tasarlanmış, saklanan bilgilerin değiştirilebildiği bilgilere erişimin, disk ya da disket sürücülerindeki erişimle karıştırılmayacak kadar hızlı olduğu bellek türüdür.[82] Tanımlardan da anlaşılacağı üzere RAM, bilgisayarın çalışır halde iken bilgileri tuttuğu elektronik bir parça olup daha iyi anlaşılabilmesi için şöyle örneklendirebiliriz[83]: boncuk ve teller ile yapılmış, sayıları toplamak için kullanılan

76 Yıldırım, "C++ Programlama, MKÜ - Bilgisayar Mühendisliği Algoritmalar ve Programlama Ders Notları", s. 4.
77 Uludoğan, a.g.e., s. 7.
78 "Bilgisayar Donanımı", s. 13, http://web.bilecik.edu.tr/bulent-turan/files/2012/10/donanim.pdf ET. 13 Ekim 2019.
79 Serpen, "Temel Bilişim Teknolojilerine Giriş", s. 34.
80 Yıldırım, "C++ Programlama, MKÜ - Bilgisayar Mühendisliği Algoritmalar ve Programlama Ders Notları", s. 6.
81 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 63.
82 İSTANBUL TEKNİK ÜNİVERSİTESİ, "Bellek Türleri", 6.09.2013, http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/bellek-turleri, ET. 13 Ekim 2019.
83 Uludoğan, a.g.e., s. 4, 5.

bir abaküste oluşturduğumuz sayıyı (723456 gibi) birkaç gün sonra tekrar baktığımızda geri okuyabiliriz, işte RAM de abaküs telleri gibi byte adı verilen bazı kutucuklardan oluşmakta ve bu kutucuklar, abaküs gibi sayıları tutmaktadır. Abaküsten farklı olarak byte adı verilen bu kutular 0 ile 255 arasında 256 farklı değer tutabilmektedir. 16 Mega Byte (MB) hafızalı bir makinada "1 Mega BYTE" yaklaşık olarak 1 milyon byte' ı ifade ettiğinden abaküsün 1 milyon telinin var olduğu düşünülebilmekte ve makinada ise 16 milyon byte büyüklüğünde hafızanın olduğu anlaşılabilmektedir.[84]

1.1.2.2.1.2.3.2. Salt Okunur Bellek (ROM- Read Only Memory)

Bilgisayarın temel işlevlerini yerine getirmesi ve açılması için gerekli olan ve bilgisayarın yapılması aşamasında üretici tarafından yerleştirilen verilerin bulunduğu bellek olup bu verilerin silinmeleri veya değiştirilmeleri veyahut güç kesintisinden dolayı zarara uğramaları mümkün değildir.[85] Başka bir ifade ile bu donanımlar bilgisayarın desteklediği komutları ve donanım bilgilerini kalıcı olarak saklayan donanımlar olup bu bilgiler üretici firma tarafından yazılıp hazır olarak ana kartla birlikte verilmektedirler.[86] ROM' da, RAM'in aksine üzerindeki bilgiler kalıcıdır, bilgisayar kapatıldığında dahi üzerindeki bilgiler gitmemektedir.[87]

1.1.2.2.1.3. Çıkış Birimleri

Bilgisayarda işlenen bilgilerin sonucunu görmemize, duymamıza veya kağıda dökmemize imkan sağlayan donanım aygıtları olup ekran (monitör), yazıcı, hoparlör, projektör, plotter gibi aygıtlardan oluşmaktadır.[88]

1.1.2.2.1.4. Saklama Birimleri

Depolama aygıtları, bilgisayara girilen ve işlenen verilerin geçici veya kalıcı olarak depolanmasını sağlayan aygıtlar olup hard disk (sabit disk), disket sürücüler, CD-DVD, flash bellekler (USB), harici diskler gibi aygıtlar saklama birimleri içerisinde yer almaktadır.[89] Sabit disk, bilgisayar üzerinde sabit olarak bulunan ve veri

84 A.e., s. 5.
85 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 63.
86 "Bilgisayara Giriş Ders Notları", s. 10.
87 "Bilgisayar Donanım Notları", s. 17, http://w3.gazi.edu.tr/~iguler/ebe250/bilg_donanim.pdf, ET. 13 Ekim 2019.
88 Ayrıntılı bilgi için bkz. a.e. s. 11-12.
89 "Bilgisayara Giriş Ders Notları", s. 10-11.

kaydetmek için kullanılan, hızlı çalışan, uzun ömürlü ve yüksek kapasiteli manyetik sığalardır.[90] [91]

1.1.2.2.2. Yazılım

Yazılım[92], verileri işlemek ve bunlardan sonuç elde etmek amacıyla bir işi bilgisayarlara yaptırabilmek için algoritma[93] şeklinde bir yazılan ve bilgisayara yapılması istenilen işlemlerden önce yüklenilen bir dizi komutu ifade etmektedir.[94] Başka bir anlatımla, bilgisayarın soyut bileşenini oluşturan, elektronik biçimde toplanabilen, depolanabilen, işlenebilen, belirli bir görevi yerine getirebilmek için bilgisayara yüklenen veya daha önce içine yerleştirilen, bilgisayara işlerlik kazandıran komutlar bütünü[95] olup sistem yazılımları ve uygulama yazılımları olmak üzere ikiye ayrılmaktadır. Yazılımın temel amacı, bilgisayarların çalışmasını kullanıcıların anlayabileceği biçime dönüştürmek ve kullanıcının verdiği komutları bilgisayar diline çevirmek olup bir işin bilgisayar ve donanımları aracılığıyla yapılabilmesini sağlayan[96] yazılım unsuru bilgisayarın temel unsurunu oluşturmaktadır.

Sistem yazılımı (system software), bilgisayarın açılmasında yüklenen, bilgisayarı hazır hale getiren, kapanana kadar görev yapan Windows, macos, Linux gibi yazılımlardır.[97] Bu yazılım türü olmaksızın bilgisayarı açılamayacağından en önemli yazılım sistemi[98] olarak görülen, bilgisayarın donanım birimleri ile kullanıcı arasında köprü görevi gören ve donanım parçalarının yönetimini sağlayan kodlardan

90 Gözü ve Aydın, a.g.e., s. 13.
91 Sabit diskler, mekanik bir sistem ile plak gibi çalışan aletler olup elektronik parçalar neredeyse ışık hızında çalışırken mekanik aletler onlara oranla otomobil hızında çalışmaktadır: bkz. Uludoğan, a.g.e., s. 6.
92 "Yazılım (software), bilgisayara yapması gerekenleri söyleyen, sabit diskte bulunan ve buradan çalıştırılan verilerdir. Bilgisayarla karşılıklı olarak bilgi alışverişini, veriyi saklamayı, korumayı ve yönetmeyi, diğer yazılımları çalıştırmayı sağlayan yazılımlar olmadan, donanım çalıştırılıp gerektiği gibi kullanılamaz. Uygulamalar (programlar), yardımcı programlar (utilities) ve işletim sistemleri en çok kullanılan yazılım örnekleridir." Bkz. Gözü ve Aydın, a.g.e., s. 15.
93 "Bilgisayarlarla beraber, çözümü algoritmik yaklaşımla tanımlama, bilgisayar bilimlerinin uygulama aracı olan, "bilgisayar programlaması yönteminin" önemli bir parçası olmuş ve bu yeni içeriği ile önemi daha da artmıştır. Bilgisayar programlaması kuramının iki kurucusu (Knuth.1969) ve (Dijkstra.1976) algoritma yaklaşımını, bilgisayar programlamasının temeli olarak tanımlarlar. Bu nedenledir ki, "bilgisayar programı makine dili ile yazılmış bir algoritma, algoritma ise konuşma dili ile yazılmış bir programdır." tanımlamaları doğrudur." bkz. N. Kaya Kılan, "Algoritma ve Harzemli (Al-Harezmi) Musa Oğlu Muhammed", *Türkiye Bilişim Ansiklopedisi*, ss. 84-86, s. 85.
94 Değirmenci, "Bilişim Suçları", s. 169; Yenidünya ve Değirmenci, a.g.e., s. 47; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 64.
95 Kurt, a.g.e., s.34.
96 "Bilgisayara Giriş Ders Notları", s. 13.
97 Akbulut, Bilişim Alanında Suçlar, s.12.
98 Yıldırım, "C++ Programlama, MKÜ - Bilgisayar Mühendisliği Algoritmalar ve Programlama Ders Notları", s. 11.

oluşan yapıları ifade etmekte olan işletim sistemidir.[99] Örneğin, cep telefonu donanım birimi olarak, sim-kart içindeki bilgiler de işletim sistemi olarak düşünülebilmektedir.[100] İşletim sistemi, donanımın doğrudan denetimi ve yönetiminden, temel sistem işlemlerinden ve uygulama programlarını çalıştırmaktan sorumlu olan sistem yazılımı olup diğer tüm yazılımların belleğe, girdi-çıktı aygıtlarına, dosya sistemine erişimini sağlamakta bunun yanında birden çok program aynı anda çalışıyorsa, her programa yeterli sistem kaynağını ayırmakta ve birbirleri ile çakışmamalarını sağlamaktadır.[101] İşletim sistemi, donanım ile kullanıcı arasındaki köprü görevi gören[102] uygulama yazılımları ise kullanıcının belli bir işi yapabilmesi ve kendisi için faydalı sonuçlar elde edebilmesi için kullanılan[103] başka bir deyişle kullanıcının bilgisayarda özel bir işlem yapabilmesini sağlayan[104], belli konulardaki problemlerin çözümüne yönelik yazılmış (Microsoft Word, İnternet Explorer, antivirüs programları gibi) programlardır.[105] "İnternet sayfalarını görüntülemek için internet Explorer, Müzik dinlemek için Winamp programı, Film izlemek için BsPlayer, Ofis uygulamaları için OpenOffice programı, Oyun oynamak için NeedforSpeed uygulama yazılımlarına örneklerdendir."[106][107] Günümüzde hemen her yazılım türü bilişim suçuna konu olmakla birlikte bilişim suçlarını işlemek için de çok sayıda farklı yazılım oluşturulmaktadır.[108]

1.1.2.3. Çalışma Sistemi

En büyük özellikleri elektronik olmaları olan[109] ve elektronik devrelerin çalışma sistemini en iyi şekilde kapsayan bir yapısının olması sebebiyle 0 ve 1 den oluşan ikili (binary) sayı sistemini kullanan dijital bilgisayarlar, veriyi elektrik sinyali olarak taşımakta ve devrenin açık veya kapalı konumuna göre bir çeşit kodlama ile

99 Emmungil, a.g.e., s. 4; Orta, a.g.e., s. 36.
100 A.e.
101 "Bilişim Teknolojileri İşletim Sitemi Temelleri", T.C. Milli Eğitim Bakanlığı MEGEP (Meslekî Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi), Ankara, 2007, s. 3, https://www.ismek.ist/files/ismekOrg/file/2013_hbo_program_modulleri/isletimsistemleritemeller.pdf, ET. 13 Ekim 2019.
102 A.e., s. 5.
103 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 65.
104 Orta, a.g.e., s. 37.
105 Akbulut, *Bilişim Alanında Suçlar*, s.12.
106 Emmungil, a.g.e., s. 5.
107 Kelime işlemciler, elektronik tablolar, sunu (presentation) programları, veri tabanı paketleri uygulama yazılımı örneklerinden olup ayrıntılı bilgi için bkz. Uludoğan, a.g.e., s. 39.
108 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 65.
109 Uludoğan, a.g.e., s. 2.

işlevini yerine getirmektedirler.[110] Duruma bağlı olarak açıkkapalı, doğru-yanlış, ve benzeri ikilemlerin karşılığını alan ve en küçük veri birimi olan bir Bit (binary digit) tek başına çok anlamlı olmadığından bilgiyi birimlendirirken bit'lerden bir grup kullanmak gerekmektedir ki bu şekilde 8 Bit bir grup oluşturduğunda bir bilgisayar bellek birimi olan Byte oluşmaktadır.[111] Bilgisayarlardaki elektronik dosyalar 0 ve 1' lerin elektronik bir oluşumu[112] olup bilgisayarlar sadece 0 ve 1' leri okuyabilmekte ve anlamlandırabilmektedir.[113] Bilgisayar tarafından alınan bütün emirler ve bilgisayara yüklenen bütün veriler sadece 1ve/veya 0 olmak üzere iki sembolü içeren sembolik bir dile çevrilmekte ve bilgisayar neyi ve nasıl yapacağı hakkında "program"[114] adı verilen kesin açıklamalar alarak çalışmaktadır.[115] Sonuç olarak özetle söylemek gerekir ise bilgisayar, elektrik devrelerinin açık ve kapalı olmasına bağlı olarak 0 ve 1 rakamlarından oluşan ikili sayı sistemine dayalı kodlama yöntemi ile çalışmaktadır.[116]

Bilgisayarın unsurları ve çalışma mantığını yukarıda ayrıntılı olarak açıklanmışsa da doktrinde bilgisayarın, diğer makinelerden ayırt edecek başka bir takım özelliklerinin bulunması gerektiğine dair görüşler ileri sürülmüştür. Yazıcıoğlu, bilgisayarın elektronik hesap makineleri ile programlanabilir aygıtlardan ayıran özelliğini, bilgisayarın bilişim (enformatik) özelliğine sahip olması yani bilgisayarın "genel amaçlı" kullanılabilme yeteneği olarak belirtmiş ve bilgisayarın yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen bir aygıt olduğunu ifade etmiştir.[117] Kurt'a göre de bilgisayarın elektronik ve manyetik

110 "Bilgisayara Giriş", s. 2.
111 A.e.
112 Karagülmez, a.g.e., s. 38.
113 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 67.
114 "Bilgisayara bir işi yaptırmak için verilen komutlar bütününe bilgisayar programı denir. Bilgisayar programı bir programlama dili kullanılarak yazılır. Program çalıştırıldığında bilgisayar ilgili komutları okuyarak programda kendisine tarif edilen işi yapar." bkz. Dülger ve Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet İletişim Hukuku (Uygulama Rehberi),* s. 26.
115 Aydın, *Bilişim Suçları ve Hukukuna Giriş*, s. 5, 6.
116 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 67,68.
117 Yazıcıoğlu bilgisayarın ayırt edici özelliğini şu şekilde açıklamaya devam etmiştir: "Öncelikle belirtmek gerekir ki, otomatiklik bilgisayarı belirleyen temel özellik değildir. Bilgisayar, her ne kadar verileri otomatik işleme tâbi tutmakta ise de, bu cihazın bilgisayar olarak nitelendirilmesine yol açan özelliği, sadece bilgileri otomatik işleme tâbi tutması değil, bu özelliğinden de faydalanılmak suretiyle genel kapsamlı olarak verileri işleyebilme, kullanabilme yeteneğidir(43), bilgi - işlem (enformatik) sürecini meydana getirmeye yarayan niteliğidir. Diğer bir ifade ile bilişim özelliğine sahip bir cihaz olması yani bilgi alıp, nakletmek, işleyebilmek bunları ifade ile bilişim özelliğine sahip bir cihaz olması yani bilgi alıp, nakletmek, işleyebilmek bunları kullanabilmek veya kullanıma sunabilmek özelliklerinin bir arada bulunduğu bir cihaz olmasıdır. Gerçekten, bilgisayarın özellikleri içinde elektronik ve manyetik olması yer almaktaysa da, ne otomatiklik, ne elektroniklik, ne manyetiklik ne de programlanabilir olmak bilgisayarı tanımlamaya yetmektedir. Zira, otomatik çamaşır makineleri, elektronik kumandalı TV.lerde de bu özellikler mevcut

olması mümkünse de bu özellikler bilgisayarı tanımlamaya yetmemekte bilgisayarın temel ayırt edici özelliğini genel kapsamlı olarak veri işleyebilme ve kullanabilme yeteneği oluşturmaktadır.[118] Dülger ise, bilgisayarın ayırt edici ögelerini bilgisayarın işletim yazılımı ya da uygulama yazılımlarının silinip üzerlerine yeni yazılımlar yüklenebilmesi ve bilgisayarın salt bir konuya özgülenmemiş yani genel amaçlı bir makine olması olarak belirtmiştir.[119]

Yukarıda yapmış olduğumuz açıklamalar ışığında, bugün için klasik dijital[120] bir bilgisayarın en önemli özelliğinin 0 ve 1' lerden oluşan bit adı verilen kodlama yöntemi ile çalışması ve özetle bilgisayarı bilgisayar yapan ana unsurların belleği ile birlikte işlemcisinin olduğunu söyleyebilmekteyiz. Zira, Ancak, teknolojide gelinen noktaya bakıldığında bir bilgisayarın hangi özelliklere sahip olması gerektiği ve hatta bir bilgisayarın diğer makinelerden ayırt edilecek başka bir takım özelliklerini sayma yolu ile ve sınırlayıcı şekilde belirlemeye çalışmak beyhude bir çabadan öteye geçemeyeceği düşünülmektedir. Nitekim, yeni nesil bilgisayarlar olarak ortaya çıkan kuantum bilgisayarlar, klasik dijital bilgisayarın çalışma ilkelerinden çok daha farklı çalışmakta olan bilgisayar modeli olarak duruma uygun güncel bir örneği oluşturmaktadır. Zira, her ne kadar şu an için "emekleme aşmasında"[121] olduğu belirtilse de gücünün ve hızının geleneksel bilgisayarlara göre çok farklı olduğu belirtilen (2019 yılının başlarında IBM tarafından da "Q System One" adı ile piyasaya sürülen[122][123]) birçok olasılık algoritmasını içinde barındıran kuantum bilgisayarlar,

bulunmaktadır(44).": bkz. Yazıcıoğlu, a.g.e., s. 58-59; Aynı yönde bkz. Tunç Demircan, *Bilişim Alanında Suçlar*, Legal Yayıncılık, İstanbul, 2016, s. 9.

118 Kurt, a.g.e., s. 29.

119 Dülger, *Bilişim Suçları*, s. 42.

120 " …Elektronik;

1. Analog (örneksel)
2. Dijital (sayısal)

olarak iki kısımda ele alınmaktadır. Analog temelli devrelerde sinyalin değişimi küçük zaman aralıklarında olmaktadır. Başka bir ifadeyle, her an sinyalin değerleri farklıdır ve sonsuz sayıda ara değer söz konusudur. Dijital özellikli devrelerde ise devreden akım geçmekte ya da geçmemektedir. Anlatımlarda akımın geçme anı (1) ile geçmeme anı ise (0) ile gösterilmektedir…

Görülüyor ki, "dijital" yapı, "elektronik" yapının kapsamı içerisinde kalmaktadır. Her dijital yapı, aynı zamanda elektroniktir; fakat her elektronik yapı aynı zamanda dijital değildir. Bu açıdan, "elektronik" kelimesi, "dijital"e göre, daha üst bir nitelik taşımaktadır…" bkz. Karagülmez, a.g.e., s. 41.

121 Mahir E. Ocak, "Kuantum Bilgisayarlar ve Kübitler", 25.03.2019, http://bilimgenc.tubitak.gov.tr/makale/kuantum-bilgisayarlar-ve-kubitler, ET. 18 Ekim 2019.

122 HÜRRİYET, "Kuantum bilgisayarlar siber güvenlikte neleri değiştirecek", 13.05.2019, http://www.hurriyet.com.tr/teknoloji/kuantum-bilgisayarlar-siber-guvenlikte-neleri-degistirecek-41211945, ET. 18 Ekim 2019.

123 "Şu anda, hiçbir kuantum bilgisayar kuantum üstünlüğünü sağlayamadı, ancak IBM hedefe çok yakın. Şirket bu yıl IBM Q System One'ın bu kritere ulaşma yönünde önemli ilerleme kaydettiğini bildirdi. (IBM Q System One, dünyanın ilk devre tabanlı ticari kuantum bilgisayarı) Cihazın hem

klasik dijital bir bilgisayarın veri kodlamada kullanmakta olduğu ikili sistemin yerine (0 ve 1) veriyi "qubit" (kübit) adı verilen birimlerle kodlamakta ve esasen uzmanlar tarafından bu bilgisayarların karmaşık sorunları geleneksel bilgisayarlara göre çok daha hızlı çözmesi beklenmektedir.[124] Teknoloji alanında bir devrim olarak gösterilen kuantum bilgisayarlar, yaratacakları etkilerle yeni bir çağ başlatmakla birlikte en iyi şifreleme tekniklerini hızlı bir şekilde aşabilmeleri nedeniyle siber saldırganlar tarafından kullanıldığında ciddi problemlere yol açabilecek[125], bu bağlamda bilişim suçları açısından suçun konusunu veya suçun işlenmesi aracını oluşturabileceklerdir. Diğer taraftan yukarıda da belirtmiş olduğumuz üzere günümüzde klasik anlamda bir bilgisayar olarak kabul edilemese de bilgisayar işlevlerini yerine getirebilen ve hatta hızla gelişen teknoloji ile bilişim suçlarının işlenmesinde araç veya suçun konusu olabilecek işletim sistemine sahip akıllı telefonlar, akıllı saatler, akıllı ev aygıtları[126], yapay zeka teknolojisine sahip ürünler, otonom araçlar gibi birçok yeni nesil cihaz[127] bulunmaktadır. Açıklamış olduğumuz hususlar ışığında doktrinde yer alan bilgisayarın diğer makinelerden ayırt edecek başka bir takım özelliklerinin bulunması gerektiği görüşlerine katılmamaktayız.

---

işlem kapasitesi hem de dengesiz kübitleri kontrol edebilme becerisi değerlendiriliyor." Bkz. Ceren Demir, "IBM, Kuantum Bilgisayarlarını En Geç 5 Yıl İçinde Piyasaya Sürmeye Hazırlanıyor", 31.05.2019, http://inovasyon101.com/kuantum-bilgisayar-ibm/, ET. 18 Ekim 2019.

124 HÜRRİYET, "Kuantum Bilgisayarlar ve Kübitler"; "Kuantum bilgisayarlar siber güvenlikte neleri değiştirecek", Hürriyetcom.tr, 13.05.2019, http://www.hurriyet.com.tr/teknoloji/kuantum-bilgisayarlar-siber-guvenlikte-neleri-degistirecek-41211945, ET. 18 Ekim 2019.

125 CYBERMAG, "Kuantum Bilgisayarlar Siber Saldırganların Eline Geçerse Ne Olur?", Bilgi Güvenliği Derneği, Sayı: 42, Temmuz 2019, s. 34.

126 " "Home Networking" teknolojisi ile geleceğin İnternet' e bağlı evlerinde tüm aygıtları birlikte çalıştırabilecek ve onları İnternet'e bağlayacak merkezi bir Ev Ağ Geçidi bulunmaktadır. Bu tarz bir ağ, çamaşır makinelerinin dinamik olarak yeni yıkama programlarını İnternet'ten indirmesini, elektronik oyuncakların üzerlerindeki oyun programlarını yenilemesini ve ev sakinleri seyahate çıkarken evdeki ütü, ışık, fırın gibi elektrikli aygıtları kapatmasını sağlayacaktır." Bkz. Hayrettin Can, Erhan Akın, "Akıllı Ev Aygıtları", *Türkiye Bilişim Ansiklopedisi,* ss. 73-78, s. 75.

127 "…ISC TURKEY 'Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nın; (www.iscturkey.org) siber güvenlik alanında 12 yıldır düzenli ve kesintisiz olarak gerçekleştirilmekte olan ülkemizdeki ilk ve tek etkinlik olduğuna vurgu yapan Alkan,… şunları aktardı: "Hayatımızın her alanına nüfuz eden internete bağlı cihazların oluşturduğu nesnelerin interneti olarak adlandırılan yeni yaşam biçimi; toplanan büyük verinin analiziyle yeni hizmetler sunulmasını sağlayarak hayatımızı kolaylaştırıp verimliğimizi artırıyor. Diğer yandan makinelar arası iletişim (M2M) ve nesnelerin interneti (IoT) gibi uygulamaların artmasıyla siber tehdit ve tehlikeler olağanüstü artış gösterirken bu durum ülkeler, kurumlar ve bireyler için hayati hale geliyor. Tüm bu büyük veri ve bilgi aktarımının ve depolanmasının güvenli bir şekilde yapılması, kriptoloji alanındaki yatırım ve çalışmalarla destekleniyor. Artık birçok kriptografik metotlar ve şifreler çözülebilir hale geldi ve yepyeni bir kavram olarak 'Post-Quantum Cryptology' (Kuantum Sonrası Kriptoloji) kavramı hayatımıza girdi. Bu alanda çok yoğun çalışmalar gerek Ar-Ge merkezlerinde gerekse de üniversitelerde başladı. Kuantum dirençli kriptografik algoritmaların ve çalışmalarının da ülkemizde yaygınlaşması çok ciddi önem arz etmekte…" bkz. Mustafa Alkan, " 'Kuantum Sonrası Kriptoloji' kavramı hayatımıza girdi", 16.07.2019, https://www.bilgiguvenligi.org.tr/kuantum-sonrasi-kriptoloji-kavrami-hayatimiza-girdi/, ET. 24 Ekim 2019.

1.1.3.Veri

Bilgi teknolojilerinde yaşanan gelişmeler neticesinde günümüzde hızla artış gösteren sayısallaşan verinin (ve bu veriden üretilen bilginin) saklanması kadar güvenliğinin sağlanması da hem bireylerin hem de devletin çok önem verdiği bir hususu oluşturmaktadır.[128] Çeşitli disiplinlerde konu üzerine çalışmalar gerçekleştirilmekte ise de çalışma konumuzu oluşturan 5237 sayılı TCK' nın "Bilişim Alanında Suçlar" bölümünde yer alan suçlar içerisinde suçun konusu olarak belirlenmiş olan verinin, esasen bilişim bilim dalı ve hatta bilişim sistemlerinin de temel yapı taşı olması[129] ve bilgi çağının yaşandığı günümüzde bilişim teknolojilerinin gelişimi ile sayısallaşan(dijitalleşen) verinin saklanması ihtiyacı yanında elektronik ortamın kendi yapısından kaynaklanan durumlar sebebiyle ortaya çıkan güvenlik ihtiyacı, verinin korunması sorunu, bilişim suçlarının artan oranda "veri güvenliği" ni hedef alması gibi sebeplerle bunun yanında bir bilişim sisteminin unsuru olması açısından da verinin, açıklanması ve tanımlanması gereken bir başka kavramı oluşturduğu düşünülmektedir. Bu bağlamda, bu başlık altında öncelikle veri kavramının sözlük tanımları, mevzuatta ve doktrinde yer alan tanımları incelenecek, TCK bağlamında veri kavramının anlamı tayin edilecektir bunun yanında benzer anlamda kullanılmakta olan fakat esasen birbirlerinden farklılıkları bulunan bilgi kavramı ile veri kavramı arasındaki ayrım belirlenerek kavram karmaşası ortadan kaldırılmaya çalışılacaktır

Her ne kadar İngilizce' de yer alan "data" ve "information" sözcükleri eş anlamlı şekilde "bilgi" sözcüğü olarak dilimize çevrilerek karışıklık yaratmakta[130] ise de İngilizce'deki "data" sözcüğünün karşılığını "veri" kelimesi oluşturmaktadır. Nitekim, İngilizce- Türkçe Ansiklopedik Bilişim Sözlüğü' nde de:

---

128 Bunun yanında çağımızın petrolü olarak değerlendirilen veriyi kullanarak bilgi üretebilir sonrasında ise değere dönüştürebilir, veriler üzerinde dönemsel davranış analizleri yapılarak geleceğe yönelik tahminler yapılabilmektedir. Dijital dönüşüm teknolojilerinden gelen, entegrasyon ve geliştirmeler ile giderek artan bir hacimde karşımıza çıkan verilerden faydalanarak analiz yapma, karar oluşturma, verilerin değerlendirilerek karar vericilere girdi oluşturmayı hedefleyen büyük veri kavramı da dijital çağın temel teknolojileri arasında yer almaktadır. Bkz. Alper Gerçek ve Haluk Gökşen, *Kobiler İçin Dijital Dönüşüm Rehberi Endüstri 4.0*, Türkiye Bilişim Derneği, Ankara Ofset, Ankara, t.y., s. 47, 48.

129 Bilişim sistemi başlığı altında ayrıntılı olarak incelenecek olsa da burada şunu belirtmekte fayda görüyoruz ki bilişim sistemi unsuru olan bilgisayar tek başına bilişim suçuna konu olabileceği gibi suçlular tarafından genellikle bilgisayar veya geniş anlamda bilişim sistemi içerisinde yer alan veriler bilişim suçuna konu olmaktadır. Bir bilişim sisteminin ise en önemli unsuru içerisinde yer alan araçlar arasında veri aktarımının sağlanması başka bir deyişle bu araçlar (bilgisayar veya bilgisayar olarak tanımlanamasa da diğer araçlar) arasında iletişimin var olmasıdır.

130 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 78, dipnot 92.

"data: veri. 1) Bir çözüme ulaşmak için işlenebilir duruma getirilmiş gözlemler, ölçümler vb. 2) Bilgisayar için işlenebilir duruma getirilmiş sayısal ya da sayısal olmayan nicelikler. 3) Olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşıma dayalı bir gösterimi"[131],

"information: bilgi, enformasyon. 1) Bilgi işlemde kabul edilmiş kurallardan yola çıkarak veriye yöneltilen anlam. 2) Bilişim kuramında, birçok olası olay arasında belirli bir olayın meydana gelme belirsizliğini, bilinemezliğini azaltan herhangi bir bilgi. 3) Bilgi işlemde, verilerden elde edilen herhangi bir kavram, olgu, anlam."[132] olarak tanımlanmıştır.

Yine, İngilizce- Türkçe Bilişim Terimleri Sözlüğü' nde veri, data kelimesinin karşılığı olarak *"İletişim, yorumlama veya işleme için uygun biçimde düzenlenmiş bilginin yeniden yorumlanabilir bir gösterimi. NOT 1: Veri insan tarafından veya otomatik olarak işlenebilir."*[133] şeklinde, bilgi ise information kelimesinin karşılığı olarak *"(Bilgi İşlemede) Belirli bir bağlamda, özel bir anlamı olan olaylar, gerçekler, işler, işlemler veya fikirler gibi kavramlar da dahil olmak üzere nesnelerle ilgili olan işlenmiş bilgi"*[134] şeklinde tanımlanmıştır. Aydın' ın Bilişim ve Telekomünikasyon Terimler Sözlüğü' nde bilgi (information), *"... 2. Kısaca, bilgi, anlam ifade etmek üzere kaydedilen, sınıflanan, organize edilen, aktarılan veya yorumlanan veriler olarak tanımlanabilir."*[135] şeklinde açıklanmıştır.[136] Türk Dil Kurumu Türkçe Sözlükte:

"veri", bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done: İstatistik veriler. 2. Bir sanat eserine veya bir edebî esere temel olan ana ilkeler: Bir romanın verileri. 3. mat. Bir problemde bilinen, belirtilmiş anlatımlardan bilinmeyeni bulmaya yarayan şey. 4. Bilişimde, olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi."[137] olarak tanımlanmıştır.

131 Sankur, a.g.e., s. 180.
132 A.e., s. 373.
133 *Bilişim Terimleri Sözlüğü İngilizce-Türkçe*, s. 52.
134 A.e., s. 105.
135 Aydın, *Telsim'in katkılarıyla Bilişim ve Telekomünikasyon Terimler Sözlüğü*, s. 432.
136 Bunun yanında "veri işlem" in karşılığı "data processing" ise, "Veriler veya temel bilgi elemanları içerin kaynak ortamlarının hazırlanması, ve belirli yöntemlerin kesin kurallarına göre, sınıflandırma, sıralama, hesaplama, özetleme ve kaydetme gibi işlemleri gerçekleştirmek üzere bu verilerin kullanılması." olarak tanımlanmıştır. Bkz. A.e, s. 189.
137 *Türk Dil Kurumu Türkçe Sözlük*, 1998, s. 2342; *Türk Dil Kurumu Türkçe Sözlük*, Hazırlayanlar: Şükrü Halûk Akalın, Recep Toparlı, Nevzat Gözüaydın, Hamza Zülfikar, Mustafa Argunşah, Nurettin Demir, Belgin Tezcan Aksu, Beyza Gültekin, 10. bsk., Türk Dil Kurumu Yayınları: 549, Ankara, 2005, s. 2087.

Laudon, "veri" kavramını *"örgütlerde veya fiziksel çevresinde gerçekleşen olayları temsil eden insanların anlayabileceği ve kullanabileceği şekilde ayarlanıp düzenlemeden önceki ham gerçekler yığınıdır."*[138] şeklinde ifade etmektedir.

Hukuk doktrininde yer alan "veri" tanımlarının birkaçına baktığımızda, Aydın, veri deyiminin, kesin ve formal biçimde yani sayılar, harfler veya diğer tipografik karakterlerle (virgül, tire vs.) ifade edilen isimler, adresler, tarihler, tutarlar, araştırma değişkenleri ve benzerinin ifade edildiğini[139] belirtmektedir. Bir başka tanımda, *"... bilgisayar tarafından iletişim, açıklama ve işlem amacıyla herhangi bir amaç, konu, durum, koşul, fikir ya da diğer unsurları açıklamak için kullanılan sayılar, harfler, simgeler belirtmek üzere kullanılan genel terim..."*[140], 'bilgilerin belli bir formata dönüştürülmüş şekli'[141], işlenmemiş ham bilgi de denilen "veri" kavramı, çeşitli durumların, gözlemlerin veya oluşumların her türlü gösterimidir.[142] Başka bir tanımda, "*bilginin sayısal koda dönüştürülmüş halidir"*[143]. Kurt ise, veriyi,

> *"bilgilerin belirli bir formata dönüştürülmüş hali olup bilginin elektriksel büyüklükle ifade edildiği, nümerik veya alfabetik nitelikteki parçacıklardan oluşan, bilgisayarın üretebileceği veya işleyebileceği, işlenebilir duruma getirilmiş sayısal ya da sayısal olmayan bilgi, olgu kavram ya da komutların iletişim işlem ve yorum için elverişli hale getirilmiş biçimsel ve uzlaşımsal gösterimi, bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan işlenmeye uygun nitelikteki her türlü bilgi konsepti"*[144]
>
> şeklinde ayrıntılı olarak açıklamıştır.

Malkoç' a göre, *"Veri kavramından, sistemce belirlenebilen her türlü işaret yanında, rakam, harf, şekillerden oluşan bilgileri anlayabiliriz."*[145] Son olarak, Dülger ise veriyi,

---

138 Kennteh C. Laudon, Jane P. Laudon, *Yönetim Bilişim Sistemleri (Dijital İşletmeyi Yönetme),* Çeviri Editörü: Uğur Yozgat, Çevirenler: Adem Öğüt, Vahap Tecim, Tunçhan Cura, Ayşe Yıldız, F. Oben Ürü, Fehmi Volkan Akyön, İbrahim Edin, İlknur Kumkale, Özlem Oktal, Ömür Yaşar Saatçıoğlu, Nihal Kartaltepe Behram, 12. Basımdan Çeviri, Nobel Akademik Yayıncılık, Ankara, 2011, s. 15.

139 Aydın, *Bilişim Suçları ve Hukukuna Giriş*, s. 3.

140 Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", *Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi*, Cilt:49, Sayı:3, Ankara, 1994, ss. 149-183, s. 169 https://dspace.ankara.edu.tr/xmlui/bitstream/handle/20.500.12575/52267/5320.pdf?sequence=1&isAllowed=y, ET. 1 Nisan 2020.

141 Mahmut Koca, "Hukukumuzda TCK' nın 244 ncü maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı, Yargıtay Başkanlığı Yayını, Ankara, 2009, s. 94 (*Aktaran* Erdoğan, Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle), s. 41)

142 Demircan, a.g.e., s. 20.

143 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 41.

144 Kurt, a.g.e., s. 37.

145 İsmail Malkoç, *Açıklamalı-İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu (Madde 179-345),* Cilt: II, 3. Bsk., Ankara, Malkoç Kitabevi, 2008, s. 2066.

"bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi"[146] olarak tanımlamaktadır.

Avrupa Konseyi Siber Suç Sözleşmesi' nde (AKSS) ise "bilgisayar verisi" terimi kullanılmış[147] ve Sözleşme' nin 1/1-b m.' sinde "bilgisayar verisi", *"bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder"* şeklinde tanımlanmıştır.[148] Ancak Dülger ise, verinin sadece "bilgisayar verisi" olarak nitelendirilmesinin bilgisayar dışında fakat bir sistemin içerisinde yer alan araçlarda bulunan verileri kapsamadığı, dolayısıyla söz konusu araçlarda bulunan verilerin suçun konusunu oluşturduğu durumlarda yaptırımsızlıkla karşılaşılabileceği gerekçesiyle sadece "veri" teriminin kullanılmasının uygun olacağını belirtmektedir.[149] Bizim de katıldığımız bu görüşe göre 5237 sayılı Türk Ceza Kanunu' nda bilişim alanında suçların sadece bilgisayar ile işlenebilen suçları içermemesi başka bir ifade ile Kanunumuzda "bilişim sistemi" nin esas alınması doğrultusunda "veri" teriminin bir türü olarak kabul edilebilecek olan "bilgisayar verisi" terimi yerine kapsayıcı ve esasen üst bir kavram olan "veri" teriminin kullanılmasının uygun olacağı düşünülmektedir.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun' un ikinci m.' sinin birinci fıkrasının k bendinde ise veri, *"Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri"*[150], bilgi ise *"Bilgi: Verilerin anlam kazanmış biçimini"*[151] ifade eder şeklinde tanımlanmıştır. Yine, 5070 sayılı Elektronik İmza Kanunu' nda "elektronik veri" terimi kullanılarak bu terimin, *"Elektronik, optik veya benzeri yollarla*

146 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 79.

147 AKSS' nin açıklayıcı raporunun 25. Paragrafında "… verilen elektronik veya diğer doğrudan işlenebilir biçimlerde olduğunu açıkça belirtmek için" "bilgisayar verisi" kavramının tercih edildiği belirtilmiştir, bkz. Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* s. 57.

148 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* s. 56.

149 Dülger ayrıca, günümüzde bilgisayarların tek başına çalıştığı gibi genellikle bir sistem dahilinde, o sistemin bir parçası olarak çalıştığını, bu sistemdeki araçların bazılarının bilgisayar tanımına uymaksızın sistemin bir parçası olarak çalışabildiği, bunlara verilebilecek en iyi örneğin üzerlerine yalnızca veri yüklenen büyük sanal bilgi depoları olduğu, bunların haricinde sistem dışında CD, taşınabilir bellek gibi veri taşıyan diğer araçların da bulunduğu, bilişim suçlarının ise büyük bir kısmının bu veriler üzerinde işlendiğini belirtmektedir. Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 79.

150 https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf, ET. 26 Ekim 2019.

151 A.e.

üretilen, taşınan veya saklanan kayıtları"[152] ifade ettiği düzenlenmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanunu' nda (KVKK) ise *"Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"*[153] ifade ettiği belirlenmiştir. Ancak şunu belirtmek gerekir ki verinin bir üst terim olduğu düşünülür ise kişisel veri verinin bir türünü oluşturmaktadır. Nitekim mevzuatımızda kişisel verilerin korunmasına yönelik doğrudan hükümler bulunmaması, mevcut bulunan hükümlerin ise kişisel verilerin korunmasına özgü felsefeden yoksun bulunması, konuya ilişkin artan ihtiyaca cevap verilmesi bunun yanında 108 sayılı Avrupa Konseyi Sözleşmesi ile 95/46 sayılı AB Direktifinin iç hukukla uyumlaştırılması amaçlarıyla[154] 6698 sayılı Kişisel Verilerin Koruması Kanunu, 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete' de yayımlanarak yürürlüğe girmiştir.[155] Ceza Hukuku bağlamında ise 765 sayılı mülga TCK' da kişisel verilerin korunması ile ilgili olarak yeterli düzenleme bulunmaması, bu verilerin izinsiz olarak işlenmesi ve başkalarına açıklanması gibi eylemlerin ceza hukukunda yeterli mücadele olanağını bulundurmaması (bu konudaki uyuşmazlıkların genellikle tazminat davalarına konu olması) 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK ile birlikte özel hayatın korunmasına dair söz konusu eksiklikler büyük ölçüde giderilerek yaptırıma bağlanmış, doğrudan doğruya kişisel verilerin korunmasına yönelik hükümler TCK' nın 135 ile 140 arasındaki m.' lerinde düzenlenmiştir.[156]

5237 sayılı Türk Ceza Kanunu' nun 243. m.' sinin gerekçesinde ise veri terimi, "sistem içindeki bütün soyut unsurlar, fıkrada geçen veri teriminin kapsamındadır" şeklinde açıklanmış[157] ve böylece Türk Ceza Kanunu bağlamında bilişim alanındaki

152 https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf, ET. 26 Ekim 2019.
153 https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, ET. 26 Ekim 2019.
154 Alaattin Bük, *Bilişim Alanında Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Ankara, 2018, s. 87, 88.
155 Bu güne kadar 2005, 2008 ve 2014 tarihli üç tasarı hazırlanmış, tasarıların hepsi de 108 sayılı Avrupa Konseyi Sözleşmesi ile 95/46 sayılı AB Direktifinden ve OECD' nin 23.09.1980 tarihli "Kişisel Alanın ve Sınır Aşan Kişisel Bilgi Trafiğinin Korunmasına İlişkin Rehber İlkeler" ile ilgili uluslararası belgelerinden büyük ölçüde esinlenmiştir. Bkz. A.e., s. 88.
"Kişisel verilerin korunması 1980'li yıllardan itibaren uluslararası sözleşmelerde yer almaya başlamıştır…Bu kapsamda Avrupa Konseyinin 28.01.1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmesi belirtilmelidir…8 Kasım 2001 tarihli Sözleşmeye Ek Protokol de bu kapsamda diğer bir düzenlemedir. Ülkemiz sözleşmeyi imzalamakla beraber 4. maddesinin zorunlu kıldığı iç hukukta kişisel verilerin korunmasına ilişkin yasanın bulunmaması nedeniyle 2016 yılına kadar TBMM tarafından onaylanamamıştır. Türkiye Sözleşmenin Onaylanmasının Uygun Bulunduğuna Dair Kanunu 18 Şubat 2016 Tarihli ve 29628 Sayılı Resmi Gazete' de yayınlamıştır…" bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 33.
156 A.e., s. 81, 82.
157 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 57.

suçlarda suçun konusunu oluşturan verinin, kapsayıcı olacak şekilde ve veri türü ayrımı yapılmaksızın geniş bir tanımı benimsenmiştir. Nitekim Kurt da, madde gerekçesinde belirtilen bu genelleme ile açıkta kalan bir husus bırakılmamaya çalışıldığını, her türlü teknolojik yenilik sonucunda ortaya çıkacak soyut unsurların "veri" kavramı kapsamına dahil edileceğinden uygulamada tanımlama sıkıntısının yaşanmamasının temin edilmeye çalışıldığını belirtmiştir.[158] Biz ise, verinin birçok tanımı bulunmakta ise de bilişim alanında ve özellikle bilişim alanında suçların konusunu oluşturan verinin, bilişim sistemleri için işlenmeye hazır ve bilişim sistemlerinin herhangi bir bölümünde yer alan (depolanan, işlenen veya iletilen) sayısal ya da sayısal olmayan her türlü unsur olduğunu kabul ederek çalışma konumuzda "veri" terimini bu anlamda incelediğimizi belirtmek istiyoruz.

Yukarıda yapmış olduğumuz açıklamalar ve tanımlar ışığında, bilişim alanındaki (bilişim haberleşme cihazları arasında gönderilen, alınan veya saklanan) verinin, ham olarak 1 ve 0' lardan oluşan bir bit dizisi olduğu[159], bilgi ve veri kavramlarının aynı olmadığı, bilgi kavramının veri kavramını da içine alan bir üst kavram olduğu, bu bağlamda önceden belirli komutların ve programların yer aldığı bilgisayar sisteminde bilginin işlenebilmesi için öncelikle veri olarak kaydedilmesi gerektiğini[160] ifade edebiliriz. Başka bir anlatımla, veri bilginin işlenmemiş ana hali olarak da ifade edilebilir. Bilgi ise, veri işlem neticesinde alıcı için bir anlam oluşturacak şekilde derlenmekte ve sunulmaktadır.[161] 1 ve 0' lardan oluşan ham haldeki bu bit dizisinin veri yapısı (formatı) değiştirilerek farklı bilgiler haline getirilebilmektedir.[162] Örneğin, 0100 0010 0100 0001 0100 0010 0100 0001 bit dizisi, veri yapısı ASCII ise "BABA", BCD ise "42414241" sayısına karşılık gelmekte ve dolayısıyla bit dizisinin anlamı doğrudan veri yapısına bağlı olarak değişmektedir.[163]

Her ne kadar çalışma konumuzu bilişim alanında suçların ceza hukuku boyutu ile incelenmesi oluştursa da bilişim alanında suçların takibi ve bu suç türleri ile

158 Kurt, a.g.e., s. 144.
159 Rifat Çölkesen, "Veri Yapıları ve Modelleri", *Türkiye Bilişim Ansiklopedisi*, ss. 892-897, s. 892.
160 Doğan, a.g.e., s. 10.
161 Aydın, *Bilişim Suçları ve Hukukuna Giriş*, s. 3.
"Veri işlem (AYDIN, E.D., 1984, s. 118) belirli verilerin toplanması, çıkarılması, çarpılması ve bölünmesini ifade eder. Bu kavram işlem için özel yardımcı araçlardan yararlanılıp yararlanılmadığına bakılmaksızın kullanılmaktadır… İş yerlerinde, devlet kurumlarında ve diğer kuruluşlarda idari işlerin büyük bir kısmı, bordrolar, muhasebe defterleri, faturalar, irsaliyeler, banka işlemleri, istatistikler gibi verilerin saklanması, çağırılması ve işlenmesinden ibarettir. Veriler elle veya bir makine aracılığı ile işlenebilir. Bilgi işlem için bilgisayar kullanıldığı takdirde elektronik bilgi işlem (EBİ) söz konusu olmaktadır." Bkz. A.e., s. 4.
162 Rifat Çölkesen, a.g.e., s. 892.
163 A.e.

mücadelede başarılı olunabilmesinin bir bütün olarak değerlendirilmesi gerektiğine inanıyoruz. Başka bir anlatımla, her ne kadar veri ve esasen üst bir kavram olan "bilgi güvenliği"[164], veriye veya bilgiye yetkisiz (izinsiz) erişimlerin vb. eylemlerin engellenmesi, verinin veya bilginin bu eylemlerden korunmasını yani suçun oluşmasından önceki önleyici aşamayı ifade etse de çalışma konumuzu oluşturan suçların engellenebilmesi veya işlenme oranlarının minimuma indirilebilmesi ve bu suçlarla etkin mücadele gerçekleştirilebilmesi için suçun oluşumundan önce "veri güvenliği" nin sağlanması, bilişim aygıtlarını kullanan bireylerin bilinçlendirilmesi ve güvenliklerini sağlayacak önlemleri almalarının sağlanması, devletin "siber güvenlik (bilişim güvenliği)"[165] stratejilerini belirleyerek ulusal siber güvenliği sağlayıcı politikalar belirlemesi, suçun tespiti, delillendirilmesi[166] ve aydınlatılması, suçun takibi ve cezalandırılması gibi aşamalar dahil bütüncül bir yaklaşımla hareket edilmesi gerektiğine inanıyoruz.

164 "Bilgi güvenliği bilginin üretilmesi, saklanması, korunması, iletişimi ve kullanılması çerçevesinde gözetilecek ilkeleri, politikaları, elektronik ve matematiksel yöntemleri içine alan bir üst kavramdır. Yirminci yüzyıla kadar bilgi güvenliği daha çok askeri ve diplomatik alanlarda önemseniyordu. Günümüzde, özellikle İnternet ve e-ticaretin yaygın kullanımı ile bilgi güvenliği yaşamsal bir önem kazanmıştır." Bkz. Fuat İnce, "Bilgi Güvenliği", *Türkiye Bilişim Ansiklopedisi,* ss. 162-166, s. 162.

165 "… bilişim suçlarının çokluğunu açıklayan faktörlerden birisi de (belki de en önemlisi), bilgi/ bilişim güvenliğinin sağlanamaması ve sorumlulukların açık bir şekilde belli olmamasıdır. Bilişim suçlarından korunmanın sağlanabilmesi yaygın şekilde desteklenen stratejileri, yeterli bilgi güvenliği, sıkı bir kanun uygulaması, teknoloji ve pazar kaynaklı çözümleri gerektirmektedir." bkz. Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 45.

Nitekim ülkemizde de sıklıkla siber güvenlikte yerli ve milli teknoloji olmadan tam bir güvenlikten bahsedilemeyeceği konuşulmakta olan bir hususdur. bkz. HÜRRİYET, "Siber savaşlara "yerli ve milli hazırlık", 25.09.2019, http://www.hurriyet.com.tr/teknoloji/siber-savaslara-yerli-ve-milli-hazirlik-41337621, ET. 26 Ekim 2019.

TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) tarafından yürütülen Pardus-Ahtapot Bütünleşik Siber Güvenlik Projesi yerli ve milli teknoloji ile üretilmiş bir sistem olarak 2016' dan beri TSK bünyesinde kullanılmaktadır. Bkz. CNNTURK, "Ahtapot yazılımı nedir, nerede kullanılıyor?" 22.12.2018 https://www.cnnturk.com/video/bilim-teknoloji/teknoloji/ahtapot-yazilimi-nedir-nerede-kullaniliyor, ET. 27 Ekim 2019.

166 "Özel inceleme ve analiz teknikleri kullanılarak bilgisayarlar başta olmak üzere, tüm elektronik medya üzerinde yer alan potansiyel delillerin toplanması amacıyla, elektronik aygıtların incelenmesi sürecine kısaca Adli Bilişim (Computer Forensic) diyoruz." Bkz. Leyla Keser Berber, "Adli Bilişim, CMK md. 134 ve Düşündürdükleri…", 10.07.2008, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html, ET. 26 Ekim 2019.

"Adli Bilişim dalı … Bilgi Teknolojileri donanım ve kaynakları kullanılarak işlenen suçları tespit edip mahkemeye / kolluk kuvvetlerine rapor şeklinde sunumunu yapıyor ve de olayların aydınlatılmasına yardımcı oluyor." bkz. Haydar Yener Arıcı, *Adli Bilişim : Kavram – Bilgiler - Uygulama Adli Bilişimde Müdahale ve Sonraki Süreçler*, 1. Bsk., Ankara, Seçkin Yayıncılık, 2018, s. 24.

1.1.4. Bilişim Ağı ve Türleri

Bilgisayarın geçirmiş olduğu tarihsel süreç ve bilgisayar sistemlerinde yaşanan teknolojik gelişmeler beraberinde bilgisayarlar arası veri iletişimi teknolojisini tetiklemiş, dağıtımlı yapıda işlenen sayısal bilginin farklı noktalar arasında iletişimi ve paylaşımı önem kazanmaya başlamıştır.[167] Zira, bilgisayarların ilk kullanılmaya başlanıldığı zamanlarda iki bilgisayar arasında veri aktarımı, diskete kopyalanarak gerçekleştirilmekte iken 80' li yıllardan sonra bilgisayarlar arasında veri iletişimi ve paylaşım ihtiyacının artmasıyla "Ağ Bağlantı Kartı" geliştirilerek bilişim dünyasına girmiş ve bilişim ağı kavramı gündeme gelmiştir.[168] Diğer bir anlatımla, tarihi süreç içerisinde bilgisayarların üretilmesiyle birlikte bilgileri aktarma yollarının daha geniş alanda kullanılmasının ve diğer bilgisayarlarla bağlantı kurularak veri alış verişinin sağlanması ihtiyacı doğrultusunda merkezi bir bilgisayara değişik sayıda terminalleri bağlamak suretiyle bilgisayar ağları kurulmaya başlanmıştır.[169]

"Birbirlerine kablolu veya kablosuz bağlanarak veri alışverişinde bulunabilen bilişim araçları ile bu imkanı sağlayan altyapı, ağ'ı (network) oluşturur."[170] Başka bir ifade ile, bilişim ağı, bilgilerin aktarımını sağlamak amacıyla birbirine hem fiziksel hem de mantıksal olarak bağlı bulunan donanım cihazlarının oluşturduğu kümeyi ifade etmektedir.[171]

Bu başlık altında, bilişim sisteminin, bilişim sistemi unsur ve araçlarının birbirleri ile iletişim kurmalarını yani birbirleri arasında veri iletişimini (aktarımını) sağlayan "ağ" kavramı incelenecektir. Doktrinde "ağ" kavramı için "bilgisayar ağı"[172], "bilişim sistem ağı"[173] gibi terimler kullanılmakta ise de esasen bu terimlerin hepsinin ifade ettiği ortak anlam "veri iletişimi" olup esasen bu iletişimin bilişim haberleşme

167 Cılız, a.g.e., s. 247.
168 Orta, a.g.e., s. 54.
169 Akbulut, *Bilişim Alanında Suçlar*, s. 15.
170 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6903
171 Orta, a.g.e., s. 55.
172 Karagülmez, a.g.e., 42; Özen ve Baştürk, a.g.e., s. 12.
Ketizmen ise "bilgisayar ya da bilişim ağı" olarak kullanmıştır bkz. Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, y.y., Adalet Yayınevi, 2008, s. 20.
Türkiye Bilişim Ansiklopedisi' nde de bilgisayar ağı kavramı kullanılmış olup "Bilgisayar ağı çok sayıda bilgisayarın karşılıklı olarak birbirlerine mesaj göndermelerini sağlayan bir yapıdır. Bu tanımda bilgisayar sözcüğü sayısallaştırılmış veri üreten, işleyen, kullanan ve saklayan her çeşit cihaz için kullanılmış bir türsel donanım soyutlamasıdır." şeklinde tanımlanarak esasen bu kavramın sadece bilgisayarlar arası iletişimi kapsamadığı vurgulanmıştır.. Bkz. A. Emre Harmancı, "Ağ Mimarisi", *Türkiye Bilişim Ansiklopedisi,* ss. 49-55, s. 49.
173 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6903; Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 25; Eker, a.g.e., s. 104.

cihaz veya donanımları ile gerçekleştiriliyor olması sebebiyle de biz "bilişim ağı"[174] terimini kullanmayı tercih etmekteyiz. Nitekim, örgütsel ölçekte bilişim sistemlerinin temelinde de çoğunlukla birbirlerinden uzak mesafede bulunan birden fazla bilgisayarın kendi aralarında veri aktarımını gerçekleştirebildikleri iletişim halinde olmaları yatmaktadır.[175] Yaşanan tarihsel süreç göz önüne alındığında bilgisayarların bilişim dünyasının temeli olması sonucunda birçok terimin bilgisayar terimi ile birlikte kullanılmakta ise de çalışma konumuzu oluşturan bilişim alanında suçların sadece bilgisayar araç olarak veya suçun konusunu oluşturarak işlenmemesi bunun yanında terminoloji bakımından da bu suçlarla uyumlu olması ve birden fazla ağ çeşidinin bulunması ayrıca hızla gelişen teknoloji neticesinde öngörülemeyen tür ve çeşitleri de kapsayıcı olması bakımından "bilişim ağı" teriminin kullanılması çalışma konumuzun daha iyi anlaşılabilmesi adına doğru bir yaklaşım olacaktır. Bu bağlamda, çalışmamız içerisinde kullanılan ve yararlanılan kaynaklarda geçen "bilgisayar ağı", kısaca "ağ" vb. ağ terimlerinin de aynı kavramı ifade ettiğinin bilinmesi gerekmektedir.

Bilişim ağının varlığından bahsedebilmek için öncelikle bilgisayarların aynı (ortak) dili kullanıyor olması, ikinci olarak da belirli kurallar ve standartlara uyulmak suretiyle kablolar veya diğer cihazlar aracılığı ile sağlanan fiziksel altyapının bulunması gerekmektedir.[176] Başka bir anlatımla, veri iletişiminin gerçekleşebilmesi, iki ucun (alıcı-verici) aynı iletişim ortamı üzerinden sinyaller alıp gönderebilmek için gerekli olan donanıma ve bu donanım üzerinden anlaşılan kurallar (protokol) dahilinde etkin iletim yapılmasına imkan sağlayacak uygulamalara sahip olmasına bağlıdır.[177] Bağlantı bakır tel, fiber optik kablolar, radyo-link sistemleri, haberleşme uyduları, kızılötesi iletişim sistemleri, radyo dalgaları ile haberleşen sistemlerden herhangi birisi ile yapılabilmektedir.[178] Bir bilgisayar ağından bahsedebilmek için esasen iki

174 Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı' nda da "bilişim ağı" terimi kullanılmış ve yasalaşmamış olan Tasarı' nın "Tanımlar" başlıklı 2. maddesinin 1. fıkrasının (e) bendinde: "Bilişim ağı : En az iki bilişim sistemi arasında veya bir bilgisayar ile bir çevre birimi arasında veri iletişimini ve karşılıklı etkileşimi her türlü iletişim tekniği ile sağlayan ortam" şeklinde tanımlanmıştır. bkz. Orta, a.g.e., s. 55, dipnot 197; https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/, ET. 27 Ekim 2019.

175 Haluk Kul, *İşletmeciler İçin Bilişim Sistemleri Temelleri ve Uygulamaları*, 1. Bs., Papatya Yayıncılık, İstanbul, 2009, s. 169.

176 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6903, 6904; Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 25, 26.

177 Ahmet Tevfik İnan, "Ağ Standartları", *Türkiye Bilişim Ansiklopedisi,* ss. 61-67, s. 61.

178 Mesih Gözüşirin, *5237 sayılı Türk Ceza Kanunu'nda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi,* Kara Harp Okulu Savunma Bilimleri Enstitüsü Güvenlik Bilimleri Anabilim Dalı Yüksek Lisans Tezi, Ankara, 2011, s. 18, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

bilgisayar ve aralarındaki "iletişim hattı"[179] yeterli iken[180] büyük ölçekte bir ağda ağ trafiğini yönetmek üzere görevlendirilen "sunucu" (veya ana makine) adı verilen bir bilgisayar, sunucuda ağ trafiğini yönetmek üzere özel bir sistem yazılımı olan Ağ İşletim Sistemi (AİS), ağa bağlı her makinede ağ içindeki bilgisayarlar ile iletişime geçebilmek için Ağ Arayüz Kartı (AAK) bulunması gerekmekte olup bilgisayarların birbirleri ile kendi aralarında bağlanmasını sağlayan "anahtar" denen aygıtlar ve var olan bilgisayar ağının diğer bilgisayar ağları ile bağlantı içinde olabilmesini sağlayan yönlendirici kullanılmalıdır.[181]

Ağ mimarisine kısaca değinmek gerekir ise, daha önce de belirtmiş olduğumuz üzere bir bilişim ağında veri iletiminin gerçekleştirilebilmesi (iletişimin sağlanabilmesi) "protokol"[182] adı verilen belirli kurallar çerçevesinde gerçekleştirilmekte, bu iletişim kuralları, veri aktarımının gerçekleştirileceği formatı, hata kontrolü esaslarını, ileti gönderimi ve alımı belirlemekte olup bilgisayar bilimlerinde birçok iletişim kuralları kümesi (en çok bilinenleri OSI ve TCP/IP başvuru modelleridir) bulunmaktadır.[183] Ağ üzerinde mesaj aktarımı bir dizi karmaşık işlevin yerine getirilmesi ile gerçekleşmekte ve bu işlevlerin yürütüldüğü sıradüzenine de katmanlı yapı adı verilmektedir.[184] ISO (International Standards Organization) tarafından önerilmiş ve 1983' te yayınlanmış olan, "protokol", hizmet vb. bir dizi kavramın sistematik olarak tanımlandığı[185] "Açık Sistemler Arabağlantısı Başvuru

179 Bilişim ağında, ağ nesneleri arasında taşınacak iletiler kablolu (fiber optik kablo vb.) veya kablosuz ortamda (yüksek frekanslı radyo, mikrodalga aktarım vb.) taşınabilmektedir. Ayrıntılı bilgi için bkz. Kul, a.g.e., s. 180-186.

180 İletişim sürecinde ileti gönderici ve ileti alıcı iki taraf bulunmakta olup göndericinin göndermek istediği iletinin düzgün bir şekilde kodlanmış ve alıcı tarafından düzgün bir şekilde çözülüp algılanmış, bu iki taraf arasında iletişimin gerçekleştiği ortam olan kanalın veri aktarımı için uygun olması başka bir anlatımla iletilerin gönderildiği kanalda gönderilecek sinyalin bilgisayarın gönderebileceği ve alabileceği sinyallerle uyumlu çalışabilmesi gerekmektedir. İletişim kanalı olarak çoğunlukla telefon hatları kullanılmakta, eski tür telefon hatlarından analog türde sinyal gönderilebildiğinden gönderici bilgisayarın dijital olarak ürettiği sinyaller "Modülatör-DEModülatör (MODEM) aracılığı ile analog sinyale dönüştürülmekte, telefon telleri ile ile aktarılan bu sinyaller diğer bilgisayara bağlı modemde dijital hale çevrilmektedir. Bilgisayarlar arasında bu haberleşmenin nasıl yapılacağına ilişkin kurallar dizisine ise "protokol" denilmektedir. Bkz. A.e., s. 169- 171.

181 A.e., s. 172.

182 "Görevdeş varlıkların birbirleriyle ilişkiye girmeleri ve karşılıklı veri alış-verişinde bulunmaları belirli kurallar içinde yapılır. Görevdeş varlıkların etkileşimi ve veri değişiminde kullanılan kurallar bütününe katman protokolü yada yalın olarak protokol denir." Bkz. Harmancı, a.g.e., s. 51.

183 Kul, a.g.e., s. 191.

184 A. Emre Harmancı, a.g.e., s. 51.

185 A.e., s. 53.

Modeli" "OSI"[186] (Open Systems Interconnection) adı verilen sistem, ağ iletişimini açıklamak için örnek bir model[187] olup bu modelde değişik katmanların birbirleriyle iletişim kurmasını sağlamak amacıyla 7 katmandan bulunmakta başka bir deyişle "iletişim 7-katmanlı bir süreç olarak tasarlanmış"[188] olup bu sistem içerisinde her katman bir üst katmana hizmet ederek verinin fiziksel katmandan başladığı yolculuğun ekranda görünen veya işlem yapılabilen sayısal varlığa dönüşmesiyle tamamlanmaktadır.[189] Günümüz ağ mimarisi ise tüm dünyada yaygın olarak kullanılan ve son yirmi yıl içinde fiili bir standart haline dönüşen, "İnternet'in iletişim kuralları kümesi"[190] olan "TCP/IP"[191] (Transmission Control Protocol/Internet Protocol-Gönderim Kontrol İletişim Kuralı/İnternet İletişim Kuralı) başvuru modelinin baskınlığı altındadır.[192]

Bilişim ağı farklı şekillerde sınıflandırılabilmekte ise de esasen yayıldıkları alan göz önüne alınarak ikiye ayrılmaktadır. Küçük bir alanda ve sınırlı sayıda cihazın birbirleriyle haberleşmesini sağlayan, "kısa mesafeli veri iletişimi"[193] sağlayan ağ türüne yerel ağ başka bir ifade ile LAN (Local Area Network/Yerel Alan Ağı) denilmektedir. Diğer bir anlatımla, birbirlerine daha yakın bilişim araçlarının belirli bir bölgede oluşturdukları ağ sistemidir.[194] Söz konusu küçük ve sınırlı alana örnek olarak ev, işyerleri, okul[195], aynı mekanda bulunan bir bina içi veya kampüs alanı[196] örnek olarak gösterilebilmekle birlikte birbirlerine yakın[197] binalar arasındaki veri aktarımı da bu ağ türüne örnek oluşturmaktadır.[198] LAN kullanımı için geliştirilen, günümüze kadar etkin ve yaygın olarak kullanılan, "ethernet" ise, önce eş-eksenel

186 OSI Modelinde katmanlar, uygulama katmanı, sunuş katmanı, oturum katmanı, ulaşım (taşıma) katmanı, ağ katmanı, veri bağı katmanı ve fiziksel katmandan oluşmaktadır. Ayrıntılı bilgi için bkz. A.e., s. 54.
187 Kul, a.g.e., s. 191.
188 A.e.
189 Orta, a.g.e., s. 55.
190 Kul, a.g.e., s. 191.
191 TCP/IP modelinde, OSI başvuru modelinde yer alan sunuş ve oturum katmanları bulunmamaktadır. Ayrıntılı bilgi için bkz. Çölkesen, a.g.e., s. 55.
192 A.e.
"TCP/IP protokolü aynı zamanda, diğer iletişim ağlarında da kullanılabilir. Özellikle pek çok farklı türde bilgisayarı veya iş istasyonlarını birbirine bağlayan yerel ağlarda (LAN) kullanımı yaygındır." Bkz. A.e., s. 455.
193 A.e., s. 247.
194 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6904.
195 Dülger ve Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet İletişim Hukuku (Uygulama Rehberi),* s. 27; Dülger ve Modoğlu, *Bilişim Suçları Modülü,* s. 57.
196 Akbulut, Bilişim Alanında Suçlar, s. 16.
197 Bazı LAN uygulamalarında farklı binalar arasında 10 kilometreye kadar yapılandırılmış ağların LAN olarak değerlendirilebildiği belirtilmektedir. Bkz. Kul, a.g.e., s. 175, 176.
198 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6904.

kablolar üzerinden, sonrasında bakır kablolar üzerinden, günümüzde ise radyo ortamında yüksek veri iletişim hızlarına erişimde kullanılan bir veri iletişim protokolü, yerel alan ağı standardıdır.[199][200] Geniş alan ağı veya WAN (Wide Area Network/Geniş Alan Ağı) ise şehir, ülke, kıta veya dünya çapındaki başka bir deyişle uzak mesafedeki cihazları birbirine bağlayan veya geniş bir alana yayılmış birden fazla yerel alan ağını içeren ağları ifade etmektedir.[201] Bu tür ağlarda mesafenin fazla olması gönderilecek sinyal ve bu bağlamda da kullanılacak aygıt türünü değiştirmekte olup mesafe ve kullanım amacına göre birkaç ülke ve hatta kıta arasında iletişim için oluşturulan "küresel ağlar"[202], belli bir kuruluşun yerel ağlarını biraraya getiren "kuruluşa yönelik ağlar", bir kuruluşun bir büyükşehir içerisinde hem LAN hem de fiber optik kablo teknolojisini kullandığı "kentsel alan ağı" ve "katma değerli ağlar" olarak ayrılmaktadır.[203] Bu yapıda iletim altyapısını kurmak ve işletmekten ulusal veya uluslararası servis sağlayıcılar sorumlu olup "ulaknet"[204] veya uluslararası nitelikteki internet, bu ağ örneklerindendir.[205]

Veri iletişiminde yaşanan bu gelişim, uzak noktalar arası iletişim gereksinimlerini de canlandırmış, bu amaçla Amerika Birleşik Devletleri' nde (ABD) savunma sektöründe yapılan araştırmalar sonucunda ortaya çıkan bir iletişim protokolü olan internetin, global bir bilgisayar ağı olarak doğmasına neden olmuş[206] olup internet bir sonraki başlıkta ayrıca incelenecektir.

Bilişim ağları içerisinde yer alan diğer ağ türlerinden "intranet" ve "sanal özel ağlar" da kısaca bahsetmekte fayda olduğunu düşünüyoruz. İntranet başka bir deyişle "iç ağ", "özel web" veya "dahili internet", "sadece belirli bir kuruluş içerisindeki

199 İnan, a.g.e., s. 62; Cılız, a.g.e., 247.

200 Günümüzde kablosuz teknolojinin yaygınlaşması ile birlikte Kablosuz Yerel Alan Ağları (WLAN) da geliştirilmiş olup birçok işletme bu hizmeti sunmaktadır. Bkz. Kul, a.g.e., s. 176.

201 Orta, a.g.e., s. 56.

Geniş alan ağında veri iletimi yöntemleri hakkında ayrıntılı bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 16.

202 İnternet, günümüzde en yaygın küresel ağ örneğini oluşturmaktadır. Bkz. Kul, a.g.e., s. 176.

203 A.e.

204 "ULAKNET; 17/07/1963 tarih ve 278 sayılı "TÜBİTAK Kurulması Hakkında Kanun"daki görevlendirme çerçevesinde, Türkiye Cumhuriyeti yasalarına ve TÜBİTAK mevzuatına uygun olarak, eğitim ve araştırma kuruluşlarının elektronik haberleşme hizmeti ve/veya elektronik haberleşme altyapısı gereksinimlerinin karşılandığı Ulusal Akademik Ağ'dır." bkz. ULAKNET, "Ulaknet Kullanım Politikası", s. 1, https://ulakbim.tubitak.gov.tr/sites/images/Ulakbim/ukp-v2011.pdf, ET. 27 Ekim 2019.

TTNet, ticari kuruluşların ve internet servis sağlayıcılarının internet omurgası ile bağlantı kurmasını sağlarken ulaknet üniversite ve akademik kuruluşların İnternet omurgasına çıkışlarını gerçekleştirmektedir. Bkz. Özen ve Baştürk, a.g.e., s. 29.

205 İnan, a.g.e., s. 65.

206 A.e.

bilgisayarları yerel ağları ve geniş alan ağlarını birbirine bağlayan ağı"[207] ifade etmektedir. Başka bir anlatımla, intranet, işyerlerinde çalışanlar arası iletişimi sağlamak ve bilgi paylaşmak amacıyla kullanılan özel bir iş ağına verilen isimdir.[208] Intranet bağlantısı birden fazla ve farklı coğrafi alanı içerisine alabilmekte fakat kısıtlı bir erişim imkanı sunabilmektedir.[209] Zira, intranetin oluşturulmasındaki temel amaç, kuruluş bünyesinde yer alan bilgileri ve bilgi işlem kapasitesini paylaşmaktır.[210] Intranet altyapı olarak internet teknolojisini kullanan[211] ancak belli bir kuruluş dışında dış dünyaya bağlantısı olmayan kapalı bir şebeke olup intranetler vasıtasıyla bir şirketin dağınık veri tabanlarına farklı noktalardan, farklı yazılım ve donanım platformları üzerinden erişim ve dahili emniyetli elektronik posta gibi uygulamalar yapılabilmektedir.[212] Belirtmiş olduğumuz gibi intranet de internetle aynı altyapıyı kullandığı için, internet üzerinde karşılaşılabilecek suçlarla intranet üzerinde de karşılaşılabilmektedir.[213] "Sanal Özel Ağlar" (Virtual Private Network) ya da kısaca "VPN" ağlara güvenli bir şekilde uzaktan erişimde kullanılan bir teknolojidir.[214] VPN, servisten faydalanan ile servisi sağlayan arasında sanal bir tünel oluşturulması suretiyle verilerin tünel aracılığı ile güvenli ve şifreli olarak gönderilerek genellikle bir veya daha fazla şirket ya da organizasyonun iletişim kurmak için internette kullanmış oldukları hususi bir iletişim ağıdır.[215] Başka bir anlatımla, VPN (Sanal Özel Ağ), bilgisayarların internet gibi genel bir ağ yapısını kullanarak kendilerine ait olan özel ağlara bağlanmasını sağlayan teknoloji altyapısı olup genel kullanıma açık olan ağ yapısını kullanıyor olmasının bir takım güvenlik endişeleri doğurması göz önünde bulundurularak bağlandığı nokta ile bilgisayar arasında adanmış ve şifreli bir tünel

207 Dülger ve Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet İletişim Hukuku (Uygulama Rehberi),* s. 27; Dülger ve Modoğlu, *Bilişim Suçları Modülü,* s. 57.
208 Akbulut, *Bilişim Alanında Suçlar,* s. 17.
209 Orta, a.g.e., s. 57.
210 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 27.
211 Başka bir anlatımla intranet, internet üzerinde geliştirilmiş standart teknolojileri ve protokolleri kullanmakta olup "TCP/IP" tabanlıdır ve yetkisiz kullanıcılardan bir firewall (güvenlik duvarı) ile korunmaktadır. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 17.
212 Sinan Ûzcan, "Güvenilir Sanal Özel İntranet", ss. 59-60, s. 59, http://www.emo.org.tr/ekler/071cfa81605a94a_ek.pdf, ET. 27 Ekim 2019.
213 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 27.
214 T.C. MİLLİ EĞİTİM BAKANLIĞI, "Bilişim Teknolojileri Ağ Temelleri", Ankara, 2011, s. 7, http://megep.meb.gov.tr/mte_program_modul/moduller_pdf/a%C4%9F%20temelleri.pdf, ET. 27 Ekim 2019.
215 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 28.

bağlantısı sayesinde bilgi akışının güvenliği arttırılmıştır.[216] VPN, internet üzerinden şifreli ve güvenli iletişimin sağlanması için düşünülmüş bir teknoloji olup kiralık hatlar (Leased-line) gibi daha sağlam ve güvenli bir çözüm yerine VPN kullanılmasındaki temel amaç maliyet, güvenlik ve kolay yapılandırma avantajlarının bir arada bulunmasıdır.[217] VPN' de veriler, VPN tünelinin bir ucunda paketlenip şifrelenmekte, diğer uçta paketler açılıp şifreler çözülerek güvenli bir şekilde iletilmekte, tünel boyunca bu süreci gerçekleştirip veri aktarımı ise "IPSec (IP Security)"[218] ve "SSL (Secure Sockets Layer/Güvenli Soket Katmanı)"[219] protokolleri ile sağlanmaktadır.[220]

Son olarak şunu belirtmek gerekir ki, bilişim sisteminin bir unsuru olan ağlarda teknolojinin ilerlemesi ile yeni çalışmalar da gerçekleştirilmektedir. Günümüzde, 5G gibi kablosuz ağlarda gerçekleşen ve nesnelerin interneti gibi yeni teknolojilerle birlikte ortaya çıkan veri artış hızı ve veri iletim hızları artışının bu verilere yönelik saldırıların da artışını ve güvenlik sorunlarını beraberinde getireceği, bu anlamda hem

---

216 Mehmet Kemal Samur ve Osman Saka, "Kampüs Ağında Sanal Özel Ağ Yapılandırması", *Akademik Bilişim'07 - IX. Akademik Bilişim Konferansı Bildirileri* 31 Ocak - 2 Şubat 2007, Kütahya, Dumlupınar Üniversitesi, ss. 267-272, s. 267, https://ab.org.tr/ab07/kitap/samur_saka_AB07.pdf, ET. 27 Ekim 2019.

217 İSTANBUL TEKNİK ÜNİVERSİTESİ, "SSL VPN (Secure Sockets Layer Virtual Private Network - Güvenli Yuva Katmanı Tabanlı Sanal Özel Ağ)", 07.09.2013, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ssl-vpn-(secure-sockets-layer-virtual-private-network---g%C3%BCvenli-yuva-katman%C4%B1-tabanl%C4%B1-sanal-%C3%B6zel-a%C4%9F), ET. 28 Ekim 2019.

218 "IPSec, şifreleme ve güvenlik hizmetlerini kullanarak IP protokollerinin güvenlik ihtiyaçlarını karşılamak için IETF (Internet Engineering Task Force – İnternet Mühendisliği Görev Gücü) tarafından geliştirilmiş bir güvenlik protokolüdür. Bu protokol sayesinde veriler ağ üzerinde güvenli bir şekilde gitmesi gereken hedeflere ulaşır. IPSec ağ katmanında çalışarak IP paketlerinin IPSec aygıtları arasında korunmasını ve kimlik denetiminin gerçekleşmesini sağlar. IPSec ağ katmanında çalıştığı için uygulamadan bağımsız olarak her veriyi şifreler ve şifre sonrası oluşturduğu başlık ile verinin İnternette rahatlıkla yolculuk edebilmesini sağlar. Bu yüzden günümüzde VPN (Virtual Private Network - Sanal Özel Ağ) teknolojisinin altyapısını oluşturmaktadır. Genellikle IPsec ile VPN kavramları birbirleriyle karıştırılır. VPN iki uç nokta arasında bir sanal ağ kurmak için kullanılır. IPSec, oluşturulan VPN bağlantılarına güvenliği arttırıcı fonksiyonlar sağlar. VPN oluşturmak için katman 2 ve katman 3 de farklı yollar mevcuttur. IPSec bu yollardan sadece bir tanesidir." bkz. İSTANBUL TEKNİK ÜNİVERSİTESİ, "IPSec VPN (Internet Protocol Security – İnternet Protokolü Güvenliği)", 07.09.2013, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ipsec-vpn-(internet-protocol-security-internet-protokol%C3%BC-g%C3%BCvenli%C4%9Fi), ET. 28 Ekim 2019.

219 "SSL, TCP katmanı ile uygulama katmanı arasında, uygulamalara uçtan uca güvenlik desteği veren bir ara katmandır…SSL tek bir protokolden oluşmaz; bir protokoller bütünüdür…" bkz. Albert Levi, "Ağ Güvenliği", *Türkiye Bilişim Ansiklopedisi*, ss. 44-49, s. 47.

220 ORTADOĞU TEKNİK ÜNİVERSİTESİ, http://cisn.odtu.edu.tr/2009-16/vpn.php, ET. 27 Ekim 2019.

"VPN' nin en önemli tercih sebebi maliyettir. Kendine ait yedekli, güvenilir, hızlı ve yüksek yatırım gerektiren bir ağa sahip olmayan kurumların, bir operatöre ait mevcut altyapıyı, kendine özel ağ gibi rahat ve güvenilir bir şekilde kullanabilmesidir." bkz. A.e.

teknik hem mevzuat anlamında ciddi çalışmalar yapılması gerektiği de hususları birçok konferansta dile getirilmektedir.[221]

1.1.5.İnternet

1.1.5.1. Genel Bilgiler

Hem LAN hem de WAN uygulamaları için kullanılabilen, "TCP/IP" olarak da adlandırılan bir veri iletişim protokolü olan internet, yeni bir devrim başlatmıştır.[222] Başka bir anlatımla, yirminci yüzyılın ikinci yarısından itibaren hayatımıza giren, telefon hatları ve TCP/IP protokolüyle tüm dünyada bulunan bilgisayar sistemlerinin birbirine bağlanması ile oluşturulan ağ olan internet zamanla hayatımızın vazgeçilemez unsurlarından olmuştur.[223] "Uluslararası ağ"[224], ""ağların ağı"[225] olarak da adlandırılan internet, birbirine bağlı ve sürekli aktif halde bulunan sunucuların (bilgisayarların) varlığı ile ayakta durmakta[226] başka bir anlatımla kendi içinde binlerce ağ ve ağların içinde de milyonlarca bilgisayar barındırmaktadır.[227] "International" ve "network" sözcüklerinin birleştirilmesi ile oluşturulan internet, bilgisayarlar arası haberleşmeyi ve iletişimi sağlayan "TCP/IP" ortak protokol dilini kullanarak bilgi alışverişinde bulunan, çeşitli ağların birleşmesi suretiyle oluşan uluslararası bir ağdır.[228] İnternet, kamuya açık olmasından ötürü bugün en yaygın ve bilinen[229] bilişim ağı olsa da bilişim ağlarının sadece bir çeşidi[230] olup "sanal alan"[231] ın sadece bir parçasını oluşturmaktadır.[232] İnternete bağlı ağların veya kullanıcıların sayısını kesin olarak bildirmek mümkün değilse de tahminlere göre internete erişim

221 BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, "Kablosuz Ağların Geleceği ve 5G'nin Önemi Konuşuldu", 30.10.2019, https://www.btk.gov.tr/haberler/kablosuz-aglarin-gelecegi-ve-5g-nin-onemi-konusuldu, ET. 23 Mart 2020.
222 Cılız, a.g.e., s. 247.
223 Kurt, a.g.e., s. 41.
224 Ali Haydar Doğru, *Bilişim Hukuku : Bilgi ve İletişim*, 2. Bsk., Ekin Yayınevi, Bursa, 2017, s. 19.
225 Yenidünya ve Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,* s. 36; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6904.
226 Doğru, a.g.e., s. 19.
227 Kul, a.g.e., s. 176.
228 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6904, 6905.
229 Özen ve Baştürk, a.g.e., s. 13.
230 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 29.
231 "Sanal alan ise, bilişim sistemleri ve bunları birbirine bağlayan her türlü veri iletim ağından oluşan, fiziksel yapısı sayısal verilerden oluşan bir alandır." bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 80.
Özen ve Baştürk, internet ağı ile birlikte tüm bilgisayar ağlarını kapsamak üzere "elektronik ortam" kavramının kullanılmasının yerinde olacağını belirtmektedir. Bkz. Özen ve Baştürk, a.g.e., s. 13.
232 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 80.

imkanı bulabilecek kişi sayısının 2020 yılına kadar 4,1 milyara çıkacağı belirtilmektedir.[233] Çalışma konumuzu oluşturan bilişim alanında suçların, internetin başka bilişim sistemlerine erişme imkanını yaratmasıdan istifade edilerek işlenebilmesini mümkün kılmaktadır.[234] Bilişim alanının en önemli unsuru olarak sayılabilecek internetin sağladığı imkan ve kolaylıklar bu sahayı geniş bir suç alanı haline getirmekle birlikte sahanın sınır tanımazlığı bu ortamda işlenen suçları da tanımaz hale getirerek büyüt boyutlu tahribatlara yol açmaktadır.[235] Kaldı ki, bilişim ağları arasında internetin bu denli yaygın kullanımı, neticesinde bilişim suçlarının işlenmesinde yaygın olarak kullanılmasını sonucunu doğurmuş ve bilişim suçlarının en karmaşık ve çözülmesi zor türlerinin çoğunlukla internet ortamında işlendiğini[236] göstermiştir. Bu bağlamda, biz de çalışmamız içerisinde interneti ayrı bir başlık altında, tanımı, tarihçesi ve (teknik) altyapısı ile ayrıca incelemeyi uygun bulduk.

1.1.5.2. Tanım

İnternet, üzerinden haberleşmenin ve/veya veri ve bilgi akışının belirli kurallar çerçevesinde sağlanabildiği merkezi olmayan ve açık bir ağ olarak da ifade edilebilmektedir.[237] Doktrinde ise:

> *'internet; birden fazla haberleşme ağının birlikte meydana getirdiği metin, resim, müzik, grafik, yazılı metin vb. gibi dosyalar ile bilgisayar yazılımlarının, kısaca insanlar tarafından oluşturulmuş her türlü bilginin veri halinde paylaşıldığı ve iletildiği bilişim sistemleri arasındaki ağ'*[238] olarak tanımlandığı gibi, *"dünya üzerinde bulunan ağların veya bilgisayarların "TCP/IP denilen yöntemle birbirine bağlanmasıyla oluşan, yeryüzündeki en büyük insan ve makine birliğini sağlayan ağa internet denir"*[239] şeklinde de tanımlanmaktadır.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun' un "Tanımlar" başlıklı ikinci m.' sinin birinci fıkrasının g ve ğ bentlerinde internet ortamı ve internet ortamında yapılan yayın terimleri kullanılmış ve bu terimler, "*g) internet*

233 Akbulut, *Bilişim Alanında Suçlar*, s. 21.
234 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6905.
235 Kurt, a.g.e., s. 46.
236 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 82.
237 Ahmet Gül, *Doğrudan/Dolaylı Bilişim Suçları*, 2. Bsk., Seçkin Yayınevi, Ankara, 2018, s. 24.
238 Ali Osman Özdilek, *İnternet ve Hukuk*, İstanbul, Papatya Yayıncılık, 2002, s. 13 (*Aktaran* Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 80); Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 29.
239 Akbulut, *Bilişim Alanında Suçlar*, s. 18.

ortamı: haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı, ğ) İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri"[240] ifade eder şeklinde tanımlanmıştır. FNC' nin (Federal Networking Council) İnternet'i tanıtan 24 Ekim 1995'te yayınladığı bir bildiride, *"İnternet, birbirilerine IP protokolüne dayalı global bir adres uzayı ile lojik olarak bağlı bilgisayarlardan oluşan bir bilgi sistemidir, TCP/IP veya benzeri IP uyumlu protokoller kullanarak haberleşmeyi sağlar ve yüksek düzeyli servislere ulaşılmasını sağlar",* şeklinde tanımlanmıştır.[241]

1.1.5.3. Tarihçe

İnternet'in tarihi oldukça karmaşık, teknolojik, yönetimsel ve toplumsal bakış açılarını içermekte dolayısıyla etkisi sadece bilgisayar haberleşmesinin teknik alanları ile sınırlı kalmayıp toplum yaşayışına yansımışsa da İnternet'in ortaya çıkısının Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan "İleri Düzey Araştırma Projeleri Kurumu" na (ARPA - Advanced Research Project Agency) dayandığı söylenebilmektedir.[242] İnternet, Amerika Birleşik Devletleri' nin olası bir savaş halinde devletin mevcut haberleşme ağlarının devamını sağlamak[243], tek bir bilgisayardan bağımsız olarak çalışabilen[244], büyük bilgisayarların güvenilir bir ağ ile birbirine bağlanması amacıyla askeri amaçlı bir proje olan "ARPANET" (The Advanced Research Projects Agency Network - Gelişmiş Araştırma Projeleri Dairesi Ağı) adlı bir bilgisayar ağını 1969' da kurması ile ortaya çıkmış, zaman içerisinde ARPANET' e farklı kuruluşların farklı türde bilgisayarlarının bağlanması ve katılımın artmasıyla büyüyerek iletişimde sorunlar oluşmaya başlamış[245],1973 yılında, ağ için bir protokol seti geliştirmek amacıyla Stanford Üniversitesi'nde bir internetworking projesi başlatılarak 1978' e kadar "İletim Kontrol Protokolü" nün (TCP - Transmission Control Protocol) dört uyarlaması denenmiş, geliştirilmiş 1980' de ise bu küme

240 https://mevzuat.gov.tr/Mevzuatmetin/1.5.5651.Pdf, ET. 29 Ekim 2019.
241 İSTANBUL TEKNİK ÜNİVERSİTESİ, "İnternet'in Tarihçesi", 07.09.2013, https://tercih.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi, ET. 29 Ekim 2019.
242 A.e.; ORTA DOĞU TEKNİK ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI, "Internet Tarihi", http://www.internetarsivi.metu.edu.tr/tarihce.php, ET. 29 Ekim 2019.
243 Geleneksel Ağ siteminde ana bilgisayar çöktüğünde ağın hiçbir işlevi kalmadığından ARPANET' in esası herhangi bir bilgisayarın devre dışı kalması halinde diğer bilgisayarların çalışmaya devam etmesidir. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 19.
244 Taşkın, a.g.e., s. 13.
245 Akbulut, *Bilişim Alanında Suçlar*, s. 19; Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 31, 32.

sabitleştirilmiş ve ARPANET' e bağlı bilgisayarlar arasındaki iletişimi kolaylaştırılmıştır.[246] 1983' te tüm ARPANET kullanıcıları "İletim Kontrol Protokolü/Internet Protokolü" (TCP/IP) olarak bilinen yeni protokole geçiş yaparak o yıl "TCP/IP", ARPANET' i de içeren Savunma Bakanlığı İnternet' inde kullanılmak üzere standartlaştırılmış[247], 1989 yılında "World Wide Web" (www) geliştirilerek internet kullanıcılarının hizmetine sunulmuş[248], Amerikan "Ulusal Bilim Vakfı" (NSF)[249], daha geniş bant kapasiteli bir global ağ sistemi olan NSFNET' i (Ulusal Bilim Vakfı Ağı) geliştirmiş, Haziran 1990 yılında dosya transfer protokolü olan "http" (hiper-text transfer protocol) geliştirilmiş[250] ve aynı yıl ARPANET kullanımdan kaldırılarak[251] NSFNET'in geliştirilmesine yönelik "İleri Ağ Hizmetleri" (ANS – Advance Network Services) birliği kurulmuş, 1995 yılı mayıs ayında NSF' nin internet omurga işletmeciliğinden çekilmesiyle ABD internet omurga işletimi tamamı ile özel işletmecilerin elinde devam etmiştir.[252] ABD' de özel şirketlerce işletilen ve hepsi "NAP" (Network Access Point – Ağ Erişim Noktası) aracılığıyla birbirine bağlı olan 11 ayrı omurga bulunmakta olup bütün ülkelerin internet ağı çıkışları bu omurgalarda bir araya getirilerek ağa bağlanan tüm bilgisayarların birbirleriyle iletişime geçmeleri bu şekilde gerçekleşmektedir.[253] ARPANET'in kaldırılmasına rağmen, "TCP/IP" protokolü günümüze kadar ve günümüzde de gelişti ve kullanılmaya devam etti.[254]

Ülkemizde ise ilk internet bağlantısı, 1993 yılında ODTÜ ve TÜBİTAK' ın ortak projesi ile ODTÜ Bilgi İşlem Daire Başkanlığı ile NSF (National Science Foundation) arasında 64 Kb/s kapasiteli bir hat üzerinden gerçekleştirilmiştir.[255]

---

246 İSTANBUL TEKNİK ÜNİVERSİTESİ, "İnternet'in Tarihçesi", https://tercih.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi, ET. 29 Ekim 2019.
247 A.e.
248 Kurt, a.g.e., s. 42.
249 Ayrıntılı bilgi için bkz. https://www.nsf.gov/about/, ET. 29 Ekim 2019.
250 Kurt, a.g.e., s. 42.
251 İSTANBUL TEKNİK ÜNİVERSİTESİ, "İnternet'in Tarihçesi", https://tercih.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi, ET. 29 Ekim 2019.
252 Akbulut, *Bilişim Alanında Suçlar*, s. 20.
253 Özen ve İhsan Baştürk, a.g.e., s. 28.
254 İSTANBUL TEKNİK ÜNİVERSİTESİ, "İnternet'in Tarihçesi", https://tercih.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi, ET. 29 Ekim 2019.
255 Pallı, a.g.e., s. 20; Mesut Orta, *Bilişim Suçlarında Adli Analiz*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Konya, 2015, s. 33, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020; Mehmet Burak Kızıltan, *5237 sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul, 2007, s. 17, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020; Gözüşirin, a.g.e., s. 20; Alper Güneş, *Bilişim Suçları ve İdarenin Hukuki Sorumluluğu*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, Yüksek Lisans Tezi, Konya, 2015, s. 9, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

1.1.5.4. İnternetin İşleyişi ve Teknik Altyapısı

Öncelikle belirtmemiz gerekir ki internete dahil olabilmemiz için bir bilişim sistemine, dijital sinyalleri analog sinyallere çeviren bir modeme, veriyi aktaracak haberleşme kanallarına ve kullanıcıların bu kanallara bağlanabilmesini sağlayacak bir İnternet Servis Sağlayıcısı' na (ISS) ihtiyaç bulunmaktadır.[256] Belirtmek gerekir ki, kendi bilgisayarlarını kullanıcıların internete ulaşabilmeleri için bir giriş kapısı olarak hizmete sunan ve kullanıcıya bir kullanıcı adı ve şifre aracılığıyla internete ulaşma imkanı sağlayan kuruluşlara internet servis sağlayıcıları denilmektedir.[257]

Yukarıda yer alan başlıklar içerisinde belirtilmiş olunduğu üzere bilgi alışverişinde bulunmayı ve bilgisayarlar arası haberleşmeyi sağlayan[258] "TCP/IP", katmanlardan oluşan ve katmanların birbiri arasında bilgi alışverişinde bulunduğu bir protokol kümesi[259] olup içerisinde "SMTP" (Simple Mail Transfer Protocol - Elektronik Posta Gönderme Protokolü), "HTTP" (Hyper Text Transfer Protokol - Hiper-Metin Transfer Protokolü), "FTP" (File Transfer Protocol - Dosya Transfer Protokolü) ve "TELNET" (Telecommunication Network – Telekomünikasyon Ağı) protokollerinin yer aldığı uygulama katmanı, "TCP" (Transmission Control Protocol – İletişim Kontrol Protokolü) ve "UDP" (User Datagram Protocol – Kullanıcı Veribloğu İletişim Kuralları) protokollerinin yer aldığı ulaşım katmanı, "IP" (Internet Protocol – İnternet Protokolü) ve "ICMP" (Internet Control Message Protocol - İnternet Kontrol Mesaj Protokolü) protokollerinin yer aldığı yönlendirme katmanı ve fiziksel katman olmak üzere dört katmandan oluşmaktadır[260].

Ulaşım katmanında yer alan "TCP" protokolü, bir üst katmandan gelen veriyi uygun büyüklükte parçalara bölüp, verinin önüne kendi başlığını eklemek suretiyle alt katmana gönderir.[261] İletilerin doğru yere ulaştırılması görevini gerçekleştirmektedir. "TCP/IP" mimarisinde 2. Katman protokolü olan "IP" protokolünün görevi ise üst katmandan gelen veriyi alıcıya uygun yoldan ve hatasız ulaştırmaktır.[262] Başka bir anlatımla, IP protokolü, kendisine gelen TCP segmentinin içinde ne olduğuyla ilgilenmeksizin veriyi ilgili IP adresine ulaştırmak için "yol" (route) bulmaktadır.[263]

256 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6905.
257 Kurt, a.g.e., s. 47.
258 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6905.
259 Özen ve Baştürk, a.g.e., s. 18.
260 Ali Efe ve Rifat Çölkesen, "Ağ Programlama ve TCP/IP", *Türkiye Bilişim Ansiklopedisi*, ss. 55-60, s. 56.
261 A.e., s. 57.
262 A.e.
263 Özen ve Baştürk, a.g.e., s. 19.

Günümüzde kullanılan IP protokolü IPv4 (IP Protokolünün 4' üncü sürümü) olup internetin hızla büyüyen adres kıtlığı problemi[264], İnternet protokollerinden sorumlu IETF' yi 1990 yıllarının başında yeni IP protokolünün geliştirilmesi amacıyla yeni bir çalışma grubu oluşturmaya sevk etti ve yaklaşık 10 yılı aşkın bir süredir endüstri, akademi, hükümetler ve çeşitli organizasyonların ortak çalışması sonucu IPv6 protokolü doğdu.[265]

Bilgisayarlar ve farklı ağlar arasında iletişim için internet ve diğer ağlar üzerinde yer alan cihazların birbirlerinden ayrı olarak belirlenebilmesi için her birinin ayırt edici bir şekilde farklı olarak isimlendirilmesi gerekmekte olup internet ağı üzerinde yer alan bir bilgisayar ya da başka bir cihazın adresine "IP adresi" (internet adresi) denilmektedir.[266] İnternet adresleri esasen 32 bitlik sayılar olup kullanıcılar tarafından birçok rakamın akılda tutulması çok zor olduğundan akılda kalacak bir

264 "Bilgisayarların iletişim sırasında uçtan uca adreslenebilmesini sağlayan IPv4 adresleri sadece 32 bitten ibarettir. 32 bitlik adres alanı teoride 4.294.967.296 tane adres yaratabilse de, verimsiz adres atama mekanizmalarından dolayı etkin adres sayısı bu noktaya hiçbir zaman ulaşamaz. WWW'in patlarcasına gelişmesinin yanı sıra son zamanlarda kablosuz erişimin de yaygınlaşmasıyla 32 bitlik adres alanı varolan ihtiyacı karşılamakta yetersiz kalmaya başlamıştır." bkz. Alper E. Yeğin, "IPv6-İnternet Protokolü Sürüm 6", *Türkiye Bilişim Ansiklopedisi*, ss. 499-503, s. 499.
"Internet'e bağlanan tüm cihazlar IP adresine ihtiyaç duyarlar. Ancak, Internet'in yaygınlaşması ve gelişen teknoloji sonrasında bu adresler hızlı bir şekilde tüketildi. Internet tarihinde, merkezi havuzda kalan son IPv4 IP bloklarının dağıtımıyla kritik bir noktaya gelindi. Bu durumu öngören uzmanlar tarafından 1996'da bir çözüm olarak sunulan IPv6, 340 trilyon kere trilyon kere trilyon adet farklı IP adresi sağlamaktadır." Bkz. ORTA DOĞU TEKNİK ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI, "IPv6 Nedir?", https://ipv6.metu.edu.tr/tr/node/1, ET. 31 Ekim 2019.
265 Efe ve Çölkesen, a.g.e., s. 57; Orhan Gökçöl ve Selvihan Nazlı Yavuzer, "İnternet Adresleri, IP ve DNS", *Türkiye Bilişim Ansiklopedisi*, ss. 455-462, s. 45; Yeğin, a.g.e., 499, 500.
"Bilgi Güvenliği Derneği Başkanı Doç. Dr. Mustafa Alkan, 4 milyar civarında olan İnternet Protokolü 4. sürümü (IPv4) adres sayısının geçen yıl Ocak ayında tükendiğini, İnternet Protokolü'nün 6.sürümüolan IPv6'ya geçişlerin başladığını bildirdi…
Bilgi ve iletişim teknolojilerinin, özellikle internetin, son yıllarda büyük bir hızla geliştiğine ve tüm dünyaya yayıldığına dikkati çeken Alkan, "Buna karşılık halihazırda yaygın olarak kullanılmakta olan IPv4, internet kullanıcı sayısının hızla artması, yeni araç ve cihazların internete bağlanmaya başlaması, yeni IP tabanlı hizmetlerin sunulması nedeniyle IP adresi ihtiyacını karşılamakta yetersiz kalmaya başladı. Ocak 2011'de IPv4 adreslerinin tükendiği ilan edildi" diye konuştu.
IPv4 adres sayısının 4 milyar civarında olduğunu anlatan Alkan, "IPv6 340 trilyon kere trilyon adres içeriyor. Dolayısıyla IP adresi neredeyse kıt kaynak olmaktan çıkıyor. Bu da her bir cihaz için statik bir IP adresi tanımlamak anlamına geliyor" dedi.
IPv6 ile artık internete bağlanan her cihazın kendine ait bir IP adresinin olacağını ifade eden Alkan, şöyle konuştu:
"Bu, internete bağlı olan tüm cihazların kimlik bilgisi olarak değerlendirilebilir. IPv6 daha fazla güvenlik seviyesi getiriyor. Dolayısıyla internet ortamında işlenen suçlar ve hacker saldırıları zorlaşacak ve internet ortamı daha güvenli hale gelecek. İnternete daha fazla sayıda ve çeşitlilikte cihaz bağlanabilecek. İnternet ortamından yeni birçok servisler ve hizmetler sağlanabilecek. İnternet ortamında işlenen suçların tespiti daha kolay olacak." " Bkz. HABERTÜRK, "IPv6'ya geçiş başladı!", 24.06.2012, https://www.haberturk.com/ekonomi/teknoloji/haber/715819-ipv6ya-gecis-basladi, ET. 31 Ekim 2019.
266 Gökçöl ve Yavuzer, a.g.e., s. 455.

adres belirlenerek, tarayıcıya bu adres yazılır ("domain name"[267] - alan adı), bu alan adı önce IP adresine çevrilir ve kullanıcı bu IP adresindeki bilgisayara yönlendirilir.[268]

"Ağ" anlamına gelen ve "World wide web" in (www) kısaltması olarak kullanılan "web" ise, yazı, resim, ses, film, canlandırma gibi farklı yapıdaki verilere erişimi sağlayan, internet üzerinde kurulmuş olan ve internetin sunduğu mekanizmaların kullanılmasını, dünya üzerindeki diğer binlerce bilgisayara bağlanmayı sağlayan genel hizmet kümesi[269], 1996' dan itibaren birbirine bağlı bilgisayarlar arasında veri paylaşımı için kuralları koyan bir işletim sistemidir.[270] Web sayfaları, kullanıcıların ağa bağlandığında erişime sunulan verilerin bilgisayar ekranında gözüktüğü[271] web uygulamaları[272] olup bir betik dili olan "HTML" ile web sayfaları yaratılmaktadır[273]. Dosyaların aktarımı için kullanılan "HTTP" ise, her türlü dosyanın Web' e aktarımı için oluşturulmuş kurallar dizini olup "bağlantı kurulması", "isteğin Web sunucusuna iletilmesi", "yanıt alma" ve "bağlantının sonlanması" olmak üzere dört aşamadan oluşan TCP/IP üzerinde çalışan bir uygulama protokolüdür.[274]

1.1.5.5. İnternetin Yönetim Biçimi ve İnternet Sujeleri

İnternet, bu sisteme giren herkesin katkısıyla oluşmuş anonim bir yapıda büyük bir ağ olup bu sistemin bir sahibi ya da yöneticisi bulunmamaktadır.[275] İnternetin, diğer tüm iletişim araçlarından ve tüm bilgisayar ağlarından farklılaştığı yönü olarak[276] belirli bir merkezinin olmayışı bir takım hukuki sorunları da beraberinde getirmektedir.[277] Başka bir anlatımla, suç oluşturan eylemleri veya kötüye kullanımları denetleyen ve bunları yargılayıp yaptırım uygulayan bir merkezi gücün bulunmayışı, bu tür olaylar gerçekleştiğinde kolluk kuvvetleri ve hukukçular için çözülmesi zor problemleri doğurmakta olup bu durumu gidermek amacıyla ülkeler internet kişiliklerinin hukuki sorumluluklarını düzenleyen yasalar yapmak ve netiket adı

267 " "İnternet alan adı" (domain name), bir web sitesi adresi içinde yer alan ve uzantılar haricindeki kısımdan oluşmaktadır, www.adalet.gov.tr, örneğinde alan adını "adalet" sözcüğü oluşturmaktadır." Bkz. Özen ve Baştürk, a.g.e., s. 20.
268 A.e.
269 Fatih Muslu, "Web: html ve http", *Türkiye Bilişim Ansiklopedisi*, ss. 917-919, s. 917.
270 A.e., s. 918.
271 Özen ve Baştürk, a.g.e., s. 24.
272 Muslu, a.g.e., s. 917.
273 A.e., s. 918.
274 A.e., s. 918, 919.
275 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 83.
276 Özen ve Baştürk, a.g.e., s. 28.
277 Taşkın, a.g.e., s. 14.

verilen kurallar oluşturmak gibi iki yol seçmektedirler.[278] Ülkemizde ise, internetin yönetimine ilişkin olarak internet süjelerinin sorumluluklarını belirlemek amacıyla 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 23/5/2007 tarihli ve 26530 sayılı Resmi Gazete' de yayımlanarak yürürlüğe girmiştir.[279]

Sanal alemi hazırlayan, sunan, sanal aleme girmemize aracılık yapan, orada kalmamızı sağlayan ve bir takım işlemler yapabilmemizi sağlayan unsurlara internet süjeleri adı verilmektedir.[280] Başka bir deyişle, internet aracılığı ile iletişim faaliyetinin gerçekleşmesi esnasında iletişim faaliyeti içinde yer alan tüm taraflara verilen isim olup[281] diğer tüm ülke içi ve dışı iletişimin sağlandığı telefon hatlarını kuran, idare eden telekomünikasyon idareleri[282], "İnternet Servis Sağlayıcıları"[283] (ISS), erişilebilen herhangi bir internet yayınının içeriğini hazırlayan veya bilgiyi bizzat üreten içerik sağlayıcılar ve bilgilerin saklandığı ve internete bağlı bulunan bilgisayarlardan ibaret hostlar[284], internet ağına erişim sağlayarak ağ üzerinde dolaşan, ağda sunulan içeriklere erişen vb. işlemleri yapabilen kullanıcılardan (browser)[285] oluşmaktadır.

1.1.6. Bilişim Alanı- Bilişim Sistemi

İlk kez 1989 tarihli Türk Ceza Kanunu Öntasarısında yer verilmiş olan[286] "bilişim alanı" kavramı, 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK' da "bilişim sistemi" kavramı yerine kullanılmakta olan[287] bir kavram olup 765 sayılı Türk Ceza Kanunu' nda yer alan 11. bapta "Bilişim Alanında Suçlar" ile 5237 sayılı Türk Ceza Kanunu' muzun "Onuncu Bölümü" nde "Bilişim Alanında Suçlar" başlığı

278 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 84, 85.
279 A.e., s. 86.
280 Kurt, a.g.e., s. 47.
281 Özen ve Baştürk, a.g.e., s. 74.
282 Kurt, a.g.e., s. 47.
283 "İnternet servis (hizmet) sağlayıcı, kullanıcıların İnternet ağına ulaşabilmeleri için kendi bilgisayarlarını bir giriş kapısı olarak hizmete sunan kuruluşlardır…
… hem 5651 sayılı Kanun ve ilgili Yönetmelik hem de 5809 sayılı Kanun'da, İSS ve erişim sağlayıcı kavramlarına birlikte yer verilmiş olması nedeniyle terminoloji birliği bulunmamaktadır." Bkz. Özen ve Baştürk, a.g.e., s. 81.
284 A.e.
5651 sayılı Kanun' un 2. maddesinin 1. fıkrasının (e) bendinde: "Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü ger-çek veya tüzel kişileri" ifade eder şeklinde tanımlanmıştır. Bkz. https://mevzuat.gov.tr/Mevzuatmetin/1.5.5651.Pdf, ET. 2 Kasım 2019.
285 Özen ve Baştürk, a.g.e., s. 83.
286 Değirmenci, "Bilişim Suçları", s. 54.
287 Malkoç bilişim sistemini bir başka ifade ile bilişim alanı olarak belirtmektedir. Bkz. Malkoç, a.g.e., s. 2065.

ile bilişim suçları düzenlenmiş olduğundan "bilişim alanı" kavramının da çalışmamızda değinilmesi gereken başka bir kavramı oluşturduğu değerlendirilmektedir.[288] Ceza mevzuatımızda yer alan bilişim alanında işlenen suçların konusunu oluşturan "bilişim sistemi" kavramı üzerinde de diğer bilişim kavramlarında olduğu gibi doktrin ve içtihatlarda farklı bir takım görüşler ileri sürülmüştür. Bu başlık içerisinde ise öncelikle bilişim alanı ve bilişim sistemi terimleri kanunda düzenleniş şekli, doktrin ve içtihatlarda getirilen yorum ve düşünceler ışığında incelenerek çalışmamızın bu bölümüne kadar yer alan başlıklarla birlikte değerlendirilerek bilişim sistemi kavramı aydınlatılmaya çalışılacaktır.

Bilişim alanı yukarıda da belirtilmiş olunduğu üzere ilk kez 1989 tarihli TCK Ön Tasarısı' nın (TCKÖT) 342. m.' sinin gerekçesinde, *'bilgileri toplayıp depo ettikten sonra bunları otomatik olarak işleme tabi tutma sistemlerinden oluşan alan'*[289] olarak belirtilmiş, bu tanım, 14.06.1991 tarihli ve 3756 sayılı "Türk Ceza Kanunu' nda Değişiklik Yapılmasına Dair Kanun" un gerekçesine de aynı şekilde aktarılmış[290], 2000 tarihli TCK Öntasarısının 345. m.' sinin gerekçesinde ise *'verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağı veren manyetik sistemlerden oluşan alan'*[291] olarak tanımlanmıştır. 2000 tarihli tasarı, 2003 yılında Meclis Genel Kurulu' na görüşülmek üzere sevk edilmiş tasarının 346. m.' sinde yer alan bilişim alanı kavramı kaldırılarak onun yerine bilişim sistemi kavramı, *'verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağı veren manyetik sistemlerden oluşan alan'*[292] şeklindeki aynı tanımlama ifadesiyle şeklinde aynı şekilde tanımlanmıştır. Şu an yürürlükte bulunan 5237 sayılı TCK' da ise suçun konusunu oluşturan "bilişim sistemi" kavramı kabul edilmiş ve 243. m.' nin gerekçesinde ise *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları*

288 Bir eylemin bilişim suçu olup olmadığını belirleyebilmek için bilişim alanını belirlemenin önemini vurgulayan bu bağlamda bir eylemin bilgisayar sistemi ile temellendirilmiş olması halinde bilişim suçu olarak kabul edilebileceği, bilgisayar sistemlerinin o eylemin gerçekleştirilmesinde yardımcı unsur olarak kullanılması halinde başka bir deyişle eylemin (faaliyetin) bilişim temelli olmaması halinde bilişim alanı olarak kabul edilemeyerek bu alanda gerçekleştirilen bir ihlalin bilişim suçu oluşturmayacağı görüşündeki yazarlar için bkz. Demircan, a.g.e., s. 8; Kurt, a.g.e., s. 26.

289 1989 Türk Ceza Kanunu Ön Tasarısı, Adalet Bakanlığı Tarafından Basılan Yayımlanmamış Metin, s. 392 (*Aktaran* Kurt, a.g.e., s. 25); Değirmenci, "Bilişim Suçları", s. 54.

290 Kurt, a.g.e., s. 25.

291 2000 tarihli TCKÖT, Adalet Bakanlığı Tarafından Basılan Yayımlanmamış Metin, s. 335 (*Aktaran* Kurt, a.g.e., s. 25)

292 2003 tarihli TCKÖT, TBMM Tarafından Basılan Yayınlanmamış Metin, s. 179 (*Aktaran* Kurt, a.g.e., s. 25)

otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir."[293] şeklinde ifade edilmiştir.

Akbulut, 3756 sayılı Kanunun tespitinin daha yerinde olduğunu, zira bilgisayar ve ona bağlı olarak çalışan sistemlerin veya bilişim sistemlerinin sadece manyetik sistemler olarak adlandırılamayacağını, manyetik sistemler yanında elektronik ve optik sistemlerin de kullanılabileceğini belirterek "bilişim alanı" kavramını şu şekilde tanımlamıştır:

> *"Bilişim alanı, verilerin işlenmesini, saklanmasını, işlenilen verilerin aktarılmasını ve bunların teknolojilerini ifade eden bir kavramdır. Bu anlamıyla iletişim ve bilgisayar dahil bütün teknolojileri içine alan bir kavramdır. Bu teknolojilerin oluşturduğu alana da bilişim alanı adı verilmektedir."*[294]

Malkoç ise, bilişim sistemi yerine bilişim alanı kavramını da kullanmakta[295] kanaatimizce Akbulut' un da belirtmiş olduğu gibi bilişim alanı veriye ilişkin gerçekleştirilen işlemlerin teknolojilerini de kapsayan bir kavramı oluşturmaktadır. Kurt ise, bilişim alanının unsurlarının tespiti ile bu sahaya ilişkin bir tanımlamanın mümkün olabileceğini, bu tanımlama yapıldığında ve sahanın sınırları çizildiğinde söz konusu sahada bilişim alanının unsurlarıyla işlenen veya bu unsurlara karşı yapılmış fiillerin bilişim suçu olarak değerlendirilebileceğini belirterek bilişim alanının unsurlarını bilgisayar ve internet olarak belirtmiştir.[296] Demircan' a göre de bir eylemin bilişim suçu olup olmadığının tespiti bakımından alanın belirlenmesi önemli olup bir faaliyetin bilgisayar sistemi ile temellenip temellenmediği, bilgisayarın o faaliyetin gerçekleşmesinde yardımcı bir unsur olarak mı kullanıldığının belirlenmesi gerekmektedir.[297] Sonuç itibariyle şu an için 5237 sayılı Türk Ceza Kanunumuzda bölüm başlığı olarak "bilişim alanı" suçun konusu olarak da "bilişim sistemi" kavramları belirlenmiş ve bilişim alanının ise yasa koyucunun iradesinin bu yönde

293 Vahit Bıçak, *Mukayeseli-Gerekçeli Türkçe- İngilizce Türk Ceza Kanunu*, 2. Bs., Seçkin Yayınevi, Ankara, 2007, s. 600.
294 Dolayısıyla Yazar' a göre makine olarak bilgisayardaki verilere veya bilgisayara karşı işlenen fiiller bilişim alanı kapsamına dahil olup, verilerin aktarılmasını sağlayan cihazlardaki veya sistemlerdeki verilere karşı gerçekleştirilen ihlaller de bilişim suçu kavramı içine girmektedir. Bkz. Akbulut, *Bilişim Alanında Suçlar*,, s. 110.
295 Malkoç, a.g.e., s. 2065.
296 Kurt, a.g.e., s. 27-47.
297 Demircan, a.g.e., s. 7, 8.

olduğu düşünülerek[298] geniş yorum yöntemi ile "bilişim olaylarının içerisinde gerçekleştiği alan"[299] olarak tanımlanabileceği kanaatindeyiz.

765 sayılı Türk Ceza Kanunu' nun bilişim suçlarını düzenleyen 525/a ile 525/d m.' leri arasında ise 5237 sayılı TCK' da kabul edilmiş olunan "bilişim sistemi" kavramı yerine "bilgileri otomatik olarak işleme tabi tutmuş olan bir sistem" ifadesi kullanılmış, madde gerekçesinde ise bu kavramın yanında ayraç içerisinde de "(bilgisayar)" kavramı belirtilmiş fakat Kanun' un içerisinde ve de gerekçesinde kavramın açıklamasına yer verilmemiştir.[300] Bu durum, her ne kadar bu kavram bilgisayar anlaşılmışsa da bilgileri otomatik işleme tabi tutan sistemden ne anlaşılması gerektiği konusunda doktrinde görüş ayrılıklarına da sebebiyet vermiştir.[301] Yargıtay,

298 Tasarıda "Bilişim Alanında Suçlar" olarak belirlenen bölüm başlığı komisyon raporunda "Bilişim Sistemlerine Karşı Suçlar" olarak değiştirilerek TBMM Genel Kurul' unda tekrar "Bilişim Alanında Suçlar" olarak değiştirilerek kabul edilmiş ve meclis tutanaklarında işlenen suçun tek başına bilişim sistemine karşı işlenmediği, aynı zamanda kuruma karşı işlenerek kişilik haklarının da çiğnendiği bu sebeplerle "Bilişim Sistemlerine Karşı Suçlar" yerine bu alanı kapsayacak genel bir değerlendirmenin uygun görüldüğü belirtilmiştir. Bkz. Karagöz, a.g.e., s. 6, 7.

299 A.e., s. 12.

300 Taşkın, a.g.e., s.6.

301 Önder' e göre, kavramda yer alan otomatik işleme tabi tutmanın mekanik bir alet içinde söz konusu olacağı fakat bilgisayarlarda asıl olanın ise elektroniklik ve manyetiklik özelliği olmaları sebebiyle kavram eleştirilmiştir. Bkz. Ayhan Önder, *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar*, İstanbul, Filiz Kitabevi, 1994, s. 505 (*Aktaran* Kurt, a.g.e., s. 140).

Ancak Akbulut ise bilgisayarların sadece elektroniklik ve manyetiklik özelliği bulunmadığı aynı zamanda optik, otomatik, vb. niteliklerinin de bulunduğu, otomatiklik özelliğinin ise sadece mekanik aletlere özgü olmayıp elektronik makinelerde de bulunduğu, bilgisayarların diğer elektronik ve mekanik aygıtlardan ayrılan özelliğinin farklı amaçlarla kullanılabilmesi olduğunu diğer araçlarda ise tüm bu özelliklerin bir arada bulunmadığı dolayısıyla otomatiklik kavramının bilgisayarları karşılamada tamamen yanlış bir ifade olmadığını belirterek Önder' in görüşünü eleştirmiştir. Ayrıca, "bilgileri otomatik işleme tabi tutmuş sistem" kavramının bilgisayarları karşılamakta tamamen yanlış bir ifade olmadığını fakat bilgisayarları anlatmak bakımından yetersiz bir ifade olduğunu belirtmektedir. Nitekim birçok araçta bilgileri depo etme, bunları işleyebilme ve anlamlı sonuçlar üretme özelliği görülmekte ise de bilgisayarları diğer elektronik ve mekanik aygıtlardan ayıran özelliğin ise veri işleme, iletme, programlanabilme ve programlarının sürekli değiştirilebilme başka bir deyişle farklı amaçlarla kullanılabilme imkanına sahip olmaları, dolayısıyla belirtilen araçların bilgisayar olarak nitelendirilemeyeceği ve bilişim suçlarının işlenmesine imkan veren bir sistem özelliğine sahip olmadıklarını, zira bunların hafızalarında bulunan sabit programlarla belirli bir amaç doğrultusunda kullanılabilmeye uygun, bilgileri aktarma özelliğine sahip olmayan cihazlar olduğu bu sebeplerle bilişim suçlarının işlendiği bilgisayarları ifade etmeyen bu kavramın daha uygun başka bir kavramla değiştirilmesinin uygun olacağını ifade etmiştir. Bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 123, 124.

Askeri Yargıtay Daireler Kurulu' nun 13.10.199497/106 sayılı kararında ise konuya ilişkin olarak 'ATM(Automatic Teller Machine:Bankamatik) makinesini bilgileri otomatik olarak işleme tabi tutan sistem kabul etmiş ve sanığı cezalandırmıştır.' Kubilay Taşdemir ve Ramazan Özkepir, *Belgelerde Sahtecilik, Mala Karşı Suçlar ve Bilişim Alanında Suçlar,* Ankara, Adil Yayınevi, 1998, s. 1117 vd. (*Aktaran* Taşkın, a.g.e., s. 8).

Şifreli yayınların izlenmesinde kullanılan decoder (şifre çözücü) cihazların bilgileri otomatik işleme tabi tutmuş sistem kavramı içinde değerlendirilip değerlendirilemeyeceği hususu, 765 sayılı TCK döneminde yoğun tartışma konularından birini oluşturmaktaydı, uygulama ve doktrinde baskın görüş ise decoderin bilgisayar kapsamında olmadığı idi, Karakehya' ya göre de bilgisayarın temel özelliği olan genel amaçlı kullanılabilme özelliğine sahip olmayıp tek amaçlı çalışma özelliğine sahip olmalarından ötürü bilgileri otomatik olarak işleme tabi tutan sistem olarak kabul

765 sayılı TCK uygulamasında, bir sistemin bilgileri otomatik işleme tabi tutan sistem olup olmadığı hususunda tereddüte düşülmesi halinde sorunun bilirkişi incelemesi yoluyla çözülmesi gerektiğini benimsemiştir.[302] Yargıtay Ceza Genel Kurulu 1996 yılında vermiş olduğu bir kararda[303], başkasının telsiz telefonunun frekansına girerek konuşmalar yapan sanığın eyleminin "bilişim alanında suçlar" başlığı altında 3756 sayılı Yasa ile yeniden düzenlenen 765 sayılı TCK' nın 525/b-2. m.' sinde tanımlanan eyleme uymadığını belirterek söz konusu fiilin 765 sayılı TCK' nın 491. m.' sinde düzenlenen hırsızlık fiilinden cezalandırılması gerektiğine hükmetmiş başka bir anlatımla Yargıtay bu kararı ile tüm elektronik aletlerin bilişim sistemi olarak kabul edilmeyeceği hususunu benimsemiştir.[304]

5237 sayılı TCK' da ise "bilişim sistemi" kavramı kabul edilerek 243. m.' sinde yer alan suç tipi içerisinde yer almıştır. Demircan' ın belirttiği üzere, eski düzenlemede yer alan "bilgileri otomatik işleme tabi tutmuş sistem" kavramı yerine doğrudan "bilişim sistemi" ifadesinin kullanılması, hukuk terminolojisindeki birliği sağlamak, yeni ve hızlı gelişen bilişim alanının müesseseleşebilmesi adına doğru bir yaklaşım olmuştur.[305] Bilişim sistemi, TCK' nın 243. m.' sinin gerekçesinde şu şekilde ifade edilmektedir: "Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tâbi tutma olanağı veren manyetik sistemlerdir."[306] Her ne kadar 5237 ile kabul edilen "bilişim sistemi" kavramı bilgisayarın yanında teknolojik gelişmeler sonucunda gelişen cihazları da kapsayacak bir üst kavram olması açısından

---

edilmemelidir. Nitekim, söz konusu fiilleri işleyenler TCK' da karşılıksız faydalanma suçuna ilişkin düzenleme sonucunda artık bu kapsamda sorumlu tutulacaktır. Bkz. Karakehya, a.g.e., s. 9, 10.

302 "…Bilişim sistemleri uzmanı olan bilirkişiye inceleme yaptırılıp, sanığın kullandığı sistemin bilgileri otomatik işleme tabi tutmuş bir sistem olup olmadığı araştırılarak, bu tür bir sistem olduğunun saptanması durumunda, sanığın teftiş raporunda belirtildiği gibi bu sistemi kullanmak suretiyle ilgili şirkete yarar sağladığı kanısına varılırsa eylemin TCY. Nın 525/b-2, 525/d ve 80. maddelerine uyan suçu oluşturacağı,…" bkz.Yargıtay 4. Ceza Dairesi, 28.02.2000 t., E:2000/1068, K:2000/1771, www.kazanci.com›kho2/ibb/giris.html, ET. 13 Temmuz 2020.

303 'Yargıtay Ceza Genel Kurulu (YCGK) 25.06.1996 tarihli ve 6/151-152' (*Aktaran* Doğan, a.g.e., s. 13, dipnot 37).

304 Kurt, a.g.e., s. 142.

305 Demircan, a.g.e., s. 65.

Hızla değişen teknoloji karşısında yetersiz kalma tehlikesi bulunan tarifler yerine daha kapsayıcı ve gelişmelere yatkı olması sebebiyle "bilişim sistemleri" kavramı doktrinde daha önceden teklif edilen bir ifade olup 5237 sayılı TCK ile nihayeten bu teklif benimsenmiştir. Bkz. Kurt, a.g.e., s. 142.

"…bilişim sistemi ibaresi, bilgisayar kavramından çok daha geniş bir kavramdır. Bu kavram bu günkü sistemleri içine alabildiği gibi, bu gün öngörülmeyen ve ileriki zamanlarda ortaya çıkacak bir kısım sistemleri de kapsayacaktır. Yine örneğin bu gün pos cihazları bilişim sistemine dahil olduğu halde, bilgisayar değildirler." Bkz. Osman Yaşar, Hasan Tahsin Gökcan ve Mustafa Artuç, *Yorumlu – Uygulamalı Türk Ceza Kanunu*, 5. Cilt, 2. Bsk., Adalet Yayınevi, Ankara, 2014, s. 7286.

306 Cumhur Şahin ve İzzet Özgenç, *Türk Ceza Hukuku Gazi Külliyatı*, Seçkin Yayınevi, Ankara, 2005, s. 321.

isabetli görülmüşse de[307] TCK' nın 243. m.' sinin gerekçesindeki tanım neyin bilişim sistemi sayılıp sayılmayacağı bunun yanında bir bilişim sisteminin hangi unsurlardan oluştuğu konusunda hukuk doktrininde farklı bir takım görüşlere yol açmıştır.

Kurt' a göre "bilişim sistemi" kavramı genel amaçlı kullanıma müsait bilgisayarları[308] ifade etmektedir.[309] Kurt' a göre:

> "*WAP (Wireless Application Protokol) Kablosuz Uygulama Protokolü sayesinde internete bağlantı yapabilen cep telefonlarının bilişim sistemi olarak kabul edilebilmesi için bu telefonların bilgisayar özelliklerine sahip olması gerekmektedir. Yani genel amaçlı işlem yapabilme özelliğine sahip bir bilgisayar ise, aynı zamanda da cep telefonu olan bu cihazı bilişim sistemi olarak kabul etmek mümkündür. Bu örnekte görüldüğü üzere telefon esasında iletişim temelli bir cihaz olmakla birlikte bilgileri otomatik olarak işleme tabi tutabilme özelliğinin kazandırılması halinde bilişim sistemi sayılabilmektedir… Arabalarda yol bilgisayarlarının kullanılması gibi veya içerisinde hangi malzemelerin bulunduğunu haber veren ve ihtiyaca göre internet sitelerinden ihtiyaç olan malzemeleri sipariş eden buzdolabı ya da her sebze ve meyveyi besin değerini kaybetmeyeceği sıcaklıklara göre pişiren bir fırın, kumaşların cinsini fark ederek ısısını ona göre ayarlayan, buhar miktarını o seviyede veren bir ütü şu an için veya pek yakında karşılaşabileceğimiz cihazlardandır. Bu cihazlar hayatın değişik sahalarında kullanılmakta bir kısım manyetik devrelerin ve programların eklenmesiyle fonksiyonları arttırılmaktadır. Bunlar bilgisayarlara ilişkin bir kısım özellikler gösterseler de genel amaçlı işlem yapamazlar, sadece kendi hafızalarına yüklenmiş bir veya iki program çerçevesinde hareket ederler. Ama bilgileri otomatik olarak işleme tabi tutan bir bilişim sistemi ise, uygun program yüklenmesiyle müzik bestelemekten en karmaşık mimari hesapların yapılmasına, grafik tasarımından istatistik sonuçları*

---

307 Bkz. Kurt, a.g.e., s. 159.

308 Aynı yönde bkz. Kubilay Taşdemir, "Türk Ceza Kanunu' nda Bilişim Suçları", *Türkiye Noterler Birliği Hukuk Dergisi*, Sayı: 129, Şubat 2006, ss. 15-28, s. 18.

309 Kurt' a göre bilişim sisteminin fonksiyonlarını yerine getirmesini sağlayan sistemin müştemilatı denilebilecek parçalarında bilişim sisteminin bir unsuru sayılması ve bunlara karşı gerçekleştirilen eylemlerin de bilişim suçu olarak değerlendirilmesi gerekir.
"…Mesela modem, ATM cihazı, post işlem makineleri, çeşitli terminaller bilişim sistemi midirler. Bu cihazlar, bilgisayar tanımlamamızdaki özellikleri taşıyan, yani çok amaçlı işlem yapabilme özelliğine sahip olan bir sisteme bağlı olarak çalışıyorsa, yani sistemin çalışmasının bir unsuru olarak faaliyet gösteriyorlarsa, bunları bilişim sisteminin bir parçası olarak göreceğiz ve bunlara karşı yapılan fiiller cezalandırma yoluna gidilecektir. Bilişim sisteminin bilgileri otomatik olarak işleme tabi tutması, manyetik olması dışında en önemli özelliği genel amaçlı kullanım özelliğidir. Yani belli bir işin yapılmasına özgülenip başka bir fonksiyon eda edemeyen bir sistem bilişim sistemi değildir. Mesela otomatik çamaşır makineleri, elektronik kumandalı TV, programlanabilen buzdolabı genel amaçlı işlem yapamadıklarından, yani yüklenen değişik programlara göre başka nitelikteki işleri yapamadıklarından bilişim sistemi olarak kabul edilemeyeceklerdir. Gerek bilişim sahasında gerekse iletişim sahasında her elektronik ve manyetik sistemin bilişim sistemi sayılmayacağı hususunu Yargıtay'da uygulamalarıyla kabul etmiştir." Bkz. Kurt, a.g.e., s. 141.

çıkarmaya kadar akla gelmeyecek çok farklı işlem yapabilir. Bilişim sisteminin neler yapabileceği programınızı ne kadar geniş bir hayal perspektifiyle ile yazığınıza bağlıdır."[310]

Ancak bu görüş Erdoğan tarafından, "genel amaçlı kullanım" ifadesinin hızlı ve sürekli gelişen teknoloji karşısında soyut ve sınırları belirsiz bir kavramı ifade etmesi, belirsiz olan bu kavramın sistemin belirlemesinde kullanılamayacağı ve ceza hukukunda bu şekilde soyut kavramlara yer verilmesinin uygun olmayacağı gerekçeleri ile eleştirilmiş, bir sistemin veri işleme, depolama ve veri iletimi özelliklerini gerçekleştirebilmesinin mümkün olması halinde bilişim sisteminin varlığının kabul edileceğini belirtmiştir.[311]

Koca-Üzülmez' e göre de insan müdahalesi olmadan otomatik işlem yapabilen, veri işleyebilen, saklayabilen, veri iletebilen ve genel amaçlı kullanılabilme özelliği olan çok yönlü fonksiyona sahip olan sistemleri bilişim sistemi olarak kabul etmek gerektiğinden veriyi toplama, işleme, çoğaltma, değerlendirme ve iletme özelliğine sahip olmayan ve sadece belirli işlemleri otomatik olarak gerçekleştiren elektronik ya da manyetik cihazlar ya da bilgiyi işleme ve iletme yeteneği olmakla birlikte bunu genel amaçlı olarak değil de tek yönlü yapabilen cihazlar (dekoder, barkot okuyucu, binalara girişi sağlayan manyetik kartlar, telefon kartları ve çamaşır makineleri gibi) 5237 sayılı TCK' nın 243. m.' sinde yer alan suçun konusunu oluşturmamakta başka bir deyişle verileri toplayabilme, saklayabilme, işleyebilme, çoğaltabilme, değerlendirebilme ve aktarabilme özelliklerinin hepsine birden sahip olan herhangi bir bilişim vasıtası bu suçun konusunu oluşturabilecektir.[312]

Taşkın' a göre de 5237 sayılı Türk Ceza Kanunu' nun 243. m.' sinde yer alan bilişim sistemi kavramının gerekçesinden yola çıkılarak bir sistemin bilişim sistemi olup olmadığı verileri gönderip alabilmesi, otomatik işlemlere tabi tutma özelliğinin bulunması, manyetik olması ile belli bir amaç için özgülenmemesi, genel amaçlı kullanılabilmesi, çok amaçlı işlem görebilmesi ölçütlerine göre belirlenecektir.[313]

---

310 A.e.

311 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 12,13.

312 Özetle, yazara göre bu cihazların bir kısmında bilgisayar özelliği bulunmakta ise de sırf tek yönlü işleve sahip olduklarından bu cihazları bilişim sistemi olarak kabul etmek mümkün değildir. Bkz. Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, 4. Bsk., Adalet Yayınevi, Ankara, 2017, s. 810-811.

313 Taşkın, a.g.e., s.10.

Taşkın' a göre "Neyin bilişim sistemi sayılacağı, neyin sayılmayacağı bakımından öğretideki bir görüş, yol gösterici olabilecektir. Bu görüşe göre bir faaliyetin bilişim faaliyeti olup olmadığı, o faaliyetin bilgisayar sistemine dahil olup olmadığına göre belirlenir. Faaliyet bilgisayar temelli

Karakehya da bilgisayarın diğer otomatik işlem yapan araçlardan ayırt eden özelliğinin, bilgileri otomatik olarak işleme tabi tutmasının yanında genel kapsamlı olarak verileri işleyebilme ve kullanılabilmesi olduğunu belirtmektedir.[314]

Ketizmen' e göre ise:

"... bilişim bilimsel bir terimdir; bilgi ya da enformasyonun özellikle elektronik araçlarla otomatik olarak işlenmesine ilişkin sürece işaret etmektedir. Bu açıdan, bilişim sistemi terimi, yukarıda aktarıldığı ve şemada örnek olarak gösterildiği üzere, bilgisayardan daha geniş bir anlama sahiptir. TCK' nin 243. vd. m.' lerinde belirtildiği şekliyle bilişim sistemi terimi de, bir bilim dalı olarak bilişimden alınmıştır. Bu durumda, maddelerde yer alan bilişim sisteminin otomatik yani insan müdahalesi olmadan işlem yapabilmesi önemli hale gelmektedir. Aynı şekilde, 243 vd. m.' lerde, veriden bahsedilmesi karşısında sistemin veri işleyebilmesi de gerekmektedir. Bu unsurları taşıyan bir sistemin, bilişim sistemi olarak kabul edilebileceğini söylemek mümkündür. Gerekçede yer alan, sistemin manyetik olması unsuru ise zorunlu bir unsur olarak kabul edilmemelidir."[315]

Artuk-Gökçen-Yenidünya ise "genel amaçlı kullanım" hususunu benimsemeden:

"... veri-işlem ve veri-iletişim unsurlarını taşıyan araçların bütününe, bilişim sistemi denilmektedir. Bu kavram; TCK.' nın 243'üncü maddesinin gerekçesinde; 'verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler' şeklinde tanımlanmıştır. Söz konusu tanım, sadece 'veri-işlemi' esas alması, 'veri-iletişimine' yer vermemesi bakımından eksiktir. Bu itibarla, bilişim sistemi yerine daha çok bilgisayarlara yönelik bir tarif getirdiğini söylemek yerinde olur. Ayrıca bilgisayarların da 'manyetik' olmak bir özelliği değildir."[316]

---

sistemle çalışmaktaysa, o sistem bilişim sistemidir. Çünkü bu durumda, bilgisayar sistemi çöktüğünde o sistem çalışamaz hale gelecektir;bankamatik makineleri buna örnek olarak verilebilir. Ancak, bilgisayar o sistemin işleyişindeki bir yardımcı unsursa, başka bir deyişle, bilgisayar olmadan da o sistem işleyebilecekse, sistem bilişim sistemi olarak tanımlanamaz; uçak firmalarının bilet satışında bilgisayar sisteminden yararlanmaları buna örnek olarak verilebilir." Bkz. A.e., s. 7.

314 "Zira otomatik çamaşır makinesi, hesap makinesi ve uzaktan kumandalı televizyonlarda da bilgileri otomatik işleme tabi tutma özelliği bulunmaktadır. Ancak bunlar genel kapsamlı olarak verileri işleyebilme özelliğine sahip olmadıklarından ve sadece tek bir amaca yönelik işlem yapabildiklerinden bilgisayar ya da bilişim sistemi sayılmazlar." Bkz. Karakehya, a.g.e., s. 8.

315 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 19.

316 Bunun yanında yazara göre "İfade edelim ki, bilişim sistemlerinin en yaygın unsuru verilerin saklanması, işlenmesi ve aktarılmasını sağlaması bakımından bilgisayarlardır. Ancak bilgisayarlar dışında da, bilişim sistemi olarak nitelendirilebilecek aygıtlar mevcuttur. Bu itibarla, bilişim suçu olarak isimlendirilen eylemler, bir bilgisayarda ya da bilgisayar olarak nitelendirilmemesine rağmen veri iletişimi sağladığı için bilişim alanına dahil unsurlardan sayılması gereken diğer elektronik, manyetik, mekanik araçlar üzerinde (örneğin, WAP uyumlu, girilen verileri saklayabilen, işleyebilen, aktarabilen cep telefonları ile üzerindeki WEB paneli sayesinde ağa bağlanıp veri aktarımı yapabilen elektronik ev aletleri) veyahut bunları veri iletişimi için birbirine bağlayan soyut

Özbek-Kanbur-Doğan-Bacaksız-Tepe' ye göre, 5237 sayılı TCK' nın 243. m.' sinin gerekçesinde yer alan tanım bilişim teknolojisinin gelişim seyri karşısında yetersiz ve muğlak görülmekte olup, öncelikle bilişim sisteminin en karakteristik özelliği olarak manyetik bir sistem olmasına dikkat çekildiği bu bağlamda manyetik olmayan bir sistemin bilişim sistemi kavramı içerisinde düşünülmesinin imkansızlaştırıldığı noktasında eleştirilmiştir. Bunun yanında "verileri toplayıp yerleştirme" ifadesinin verileri kimin toplayacağı ve nereye yerleştireceğinin belirli olmaması açısından muğlak kaldığına vurgu yapılmış, TCK' nın 243. m.' si anlamında bilişim sistemi kavramının sadece bilgisayar veya internet gibi sistemlere indirgenmeden bu sistemler de dahil olmak üzere bir bütün olarak ele alınması gerektiği belirtilmiştir.[317]

Yargıtay Ceza Genel Kurulu ise, sanığın telefon klübelerinden topladığı kredisi bitmiş telefon kartlarına barkod ve manyetik bant yapıştırmak suretiyle kontör yükleyip bunları diğer sanık ile birlikte katılan Kurum' a ait kulübelerde bulunan telefon cihazlarına sokarak kullanmaları ve toplam 35210 kontörlük görüşme yapmalarına ilişkin eylemlerine ilişkin 2007 yılında vermiş olduğu kararında[318] genel amaçlı kullanım ölçütünü belirlemiş[319] ve

> *"... Somut olayda sanığın, kredisi bitmiş olan manyetik telefon kartları üzerinde yaptığı değişikliklerle, sistemin verileri farklı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklenmesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan 765 sayılı Türk Ceza Yasası'nın 525 b maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı*

---

veya somut ağlar üzerinde işlenebilir." Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6902.
aynı yönde görüşler için bkz. Değirmenci, "Bilişim Suçları", s. 54; Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 17.
317 Veli Özer Özbek, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, *Türk Ceza Hukuku Özel Hükümler*, 9. bsk., Seçkin Yayıncılık, Ankara, 2015, s. 920.
318 Koca-Üzülmez, Yargıtay CGK' nın vermiş olduğu karara katılmadıklarını belirtmiştirler. Şöyle ki: "Yargıtay CGK bu kararında telefon kulübelerinden toplanan kredisi bitmiş telefon kartlarına barkot ve manyetik bant yapıştırmak suretiyle kontör yükleyip telefon görüşmesi yapılmasını bilişim sistemlerini kullanarak haksız yarar sağlama suçu (m. 244/4) kapsamında değerlendirmiştir. Bu karara muhalif kalan kurul üyelerinin de belirttikleri gibi, manyetik telefon kartlarının kendisi bir bilişim sisteminde bulunması gereken özelliklere sahip olmadığı gibi, bu kartlar kullanılarak bir bilişim sistemine bağlanılması da söz konusu değildir. Bu nedenle yalnızca telefon makinesini görüşmeye açan manyetik telefon kartları bu suçun konusunu oluşturmazlar. Bu tür fiiller karşılıksız yararlanma suçunu (m.163) oluştururlar." Bkz. Koca ve Üzülmez, a.g.e., s. 811, dipnot: 30.
319 Yargıtay Ceza Genel Kurulu, 10.06.2007 t., E: 2007/6-136 E., K: 2007/150, www.kazanci.com›kho2/ibb/giris.html, ET. 13 Temmuz 2020.

yarar sağlamak suçunu, gerekse suçtan sonra yürürlüğe giren 5237 sayılı Türk Ceza Yasası'nın 244. maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır. Uygulamada hangi Yasa' nın daha lehe sonuç verdiği hususu da Yerel Mahkemece değerlendirilip saptanmalıdır."[320]

kararına hükmetmiştir.[321]

"Bilişim sistemi" kavramı 20.09.2011 tarihli ve 28060 sayılı Resmi Gazete' de yayınlanan Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik' in "Tanımlar ve kısaltmalar" başlıklı 3' üncü m.' sinin birinci fıkrasının b bendinde: *"Bilişim sistemi: Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi"*[322] ifade eder şeklinde tanımlanmıştır. Avrupa Konseyi Siber Suçlar Sözleşmesi' nde (AKSS) ise "bilgisayar sistemi" kavramı yer almakta olup Sözleşmenin "Tanımlar" başlıklı birinci m.' sinde *"bilgisayar sistemi terimi, bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbirleriyle bağlantılı veya ilgili bir grup cihazı ifade eder"*[323] şeklinde tanımlanmıştır. İngilizce-Türkçe Ansiklopedik Bilişim Sözlüğü' nde "information system" olarak ifade edilen bilişim sistemi terimi, *"Belli bir konuya ya da örgüte ilişkin verilerin bir düzen içinde bilgisayar ortamında saklandığı ve kullanıcılara*

320 "Ankesörlü telefonlar, manyetik kart, kredi kartı ve smart kart ile çalışan hizmet telefonlarıdır. Bu telefonlar katılan Kurum tarafından ücretsiz olarak meydanlar, hastaneler, terminaller, garlar, limanlar, metro istasyonları, askeri tesisler, Toplu konut alanları gibi halka açık yerlere tesis edilmekte, ARMS olarak adlandırılan merkezi bilgisayar sistemi ile yönetilmektedir. ARMS sisteminin, suçun işlendiği bölgede hizmet veren ve kendisine bağlı olan 200 adet D-3 manyetik kartlı ankesör makinesinin çalışma bilgilerini, (kullanılan kontör miktarı, manyetik karta ait barkot numaraları, görüşen ve görüşülen bölgeler ve numaralar, görüşme saati ve süresi v.s) bünyesinde tokatladığı anlaşılmaktadır. Nitekim kopyalama yapılan manyetik kartların barkot numaraları dahi bu sayede tespit edilebilmiştir. Suç tarihinde kullanılan sistemin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura ihtiyaç vardır.
Bunlardan birincisi, manyetik telefon kartı, diğeri ise kontör olarak adlandırılan kredidir. Bunlara sahip olunmadan, bir bilgi işlem biriminin parçası olan ve ARMS denilen sisteme bağlı bulunan ankesörlü makinelerden, Kurum'ca acil durumlarda kredisiz görüşme yapılabilmesine olanak sağlanmış bulunan sınırlı sayıdaki numara dışında görüşme yapılabilmesine olanak yoktur. Bu sistemde, manyetik kart üzerindeki barkodu okuyan makine, manyetik kart üzerinde kullanılmış kredi bilgileri bulunmadığı takdirde, okuduğu kartın kredi sınıflandırma özelliklerine göre 100, 60 veya 30 kontör kredi yüklemesi yapmak suretiyle kullanıma hazır hale getirmekte, kullanım süresince yaptığı hesaplamaların sonucuna göre kalan kredi miktarını saptayıp manyetik karta işlemektedir. Başka ifadeyle sistem, makineye takılan karttaki verilerin alınıp değerlendirilmesi suretiyle işlemektedir." Bkz. Yargıtay Ceza Genel Kurulu, 10.06.2007 t., E: 2007/6-136 E., K: 2007/150, www.kazanci.com›kho2/ibb/giris.html, ET. 13 Temmuz 2020.

321 Yargıtay' ın ATM' lerin bilgileri otomatik işleme tabi tutan sistem olduğunu kabul ettiği karar için bkz. Yargıtay Ceza Genel Kurulu, 10.04.2001, E: 2001/6-30, K: 2001/57, www.kazanci.com›kho2/ibb/giris.html, ET. 13 Temmuz 2020.

322 https://resmigazete.gov.tr/eskiler/2011/09/20110920-4.htm, ET. 1 Nisan 2020.

323 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, Yasama Dönemi: 24, Yasama Yılı: 3, Sıra Sayısı: 380, s. 14, https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, ET. 20 Ekim 2019.

gereksindikçe raporlar üreten ya da gereksenen veriye kabul edilebilecek kısa bir süre içinde erişim olanağı sağlayan yazılım ve veriler topluluğu"[324] olarak tanımlanmıştır. "Bilgisayar sistemi" (computer system) ise *"Yazılım hariç bir bilgisayarı oluşturan donanım birimlerinin topluluğu. Bir kişisel bilgisayar klavye, monitör, disk sürücüleri, bazen de modemden bir bilgisayar sistemine örnektir."*[325] şeklinde tanımlanmıştır.

Dülger ve Modoğlu ise bilişim sistemini,

> *"Bilgisayar çevre birimleri (bir bilgisayarın çalışması için zorunlu olmayan ancak kullanımını kolaylaştıran hoparlör, CD ROM, Mouse, klavye, kulaklık, yazıcı vb), iletişim altyapısı (elektronik haberleşme, internet, intranet gibi) ve programlardan oluşan veri işleme saklama ve iletmeye yönelik sistemi ifade eder."*[326] şeklinde tanımlamaktadır.

Bük ise bilişim sisteminin en basit ifadeyle elektronik makineler olduğunu, bu makinelerin veri veya bilgilerin kaydedildiği ve bu verilerin işleme tabi tutulabilen, sonuçları ya da verileri çıktı şeklinde verebilen cihazlar olduğunu belirtmektedir.[327]

Bir kavram olarak sistem; bir sonuç elde etmeye yarayan, girdiler alıp çıktılar oluşturan, organize bir dönüşüm süreci ile ortak bir amaca yönelik beraber çalışan ve birbirleriyle ilişkili elemanların doğal ve yapay olarak oluşturduğu grup olup bilişim sistemleri, bilgi yönetiminin ortak amaçlarını gerçekleştirebilmek için insan, veri, prosedürler, donanım ve yazılımın birlikte oluşturduğu; verilerin belirli bir amaç doğrultusunda toplanması, depolanması, işlenmesi ve iletilmesini sağlayan sistemlerdir.[328] Başka bir anlatımla, bilişim sistemi, bir organizasyonda karar verme sürecine katkıda bulunmak için verileri toplayan, bilgiye dönüştüren, saklayan ve dağıtan birbirine bağımlı ögelerin toplamı olup bilişim sistemleri, en basit anlamda amacı bilgiyi kaydetmek, işlemek ve dağıtmak olan bir sistemdir.[329] Bilişim sistemleri

---

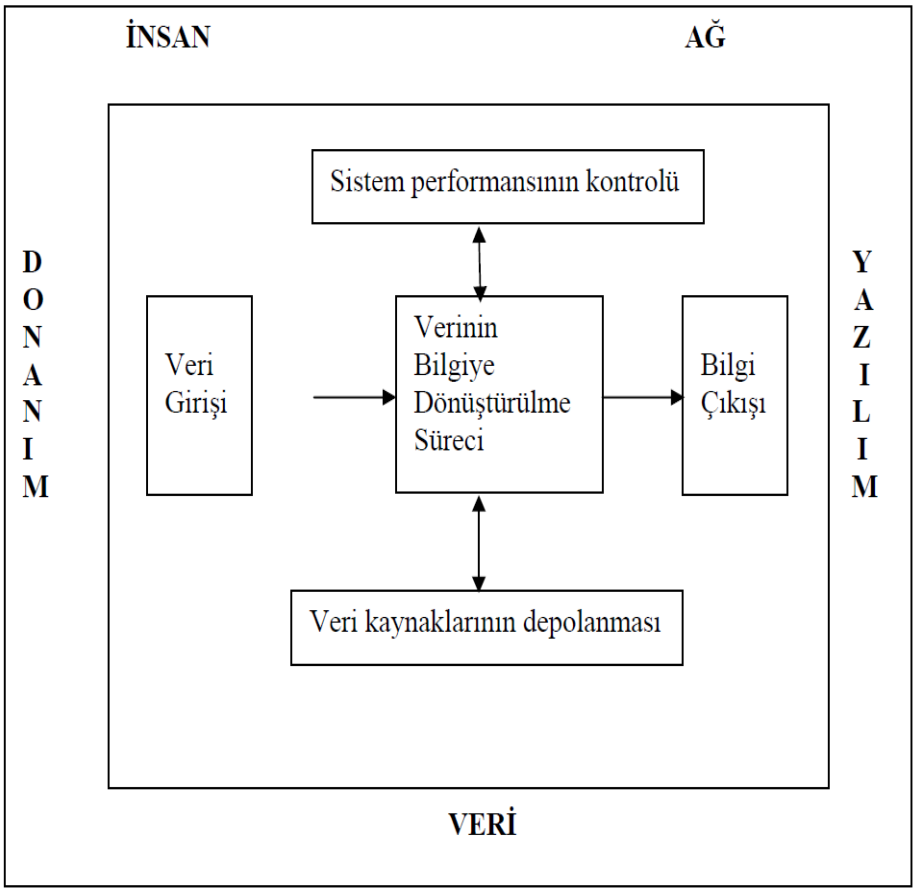
324 Sankur, a.g.e., s. 375.
325 A.e., s.145.
326 Dülger ve Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet İletişim Hukuku (Uygulama Rehberi)*, s. 25.
327 Bük' e göre burada bilişim sistemi olarak sadece bilgisayarlardan söz edildiğinin kabulü yanıltıcı olacaktır. Zira, bu durumun kabulü halinde verilerin depolanması, işleme tabi tutulması veya nakledilmesindeki modem, ATM cihazları, benzeri işlem makineleri gibi pek çok yazılım kullanan cihaza yönelik fiiller bilişim alanında suç sayılamayacaktır. Oysa TCK' nın konu başlığı bilgisayarı değil daha üst kavram olan bilişim sistemini işaret etmektedir. Bkz. Bük, a.g.e., s. 51.
328 Ahmet Fatih Özyılmaz, *Bilişim Sistemleri, Sağlıkta Bilişim Sistemleri ve Performans*, Beykent Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı Hastane ve Sağlık Kurumları Yönetimi Bilimdalı, İstanbul, 2014, s. 9, 11, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.
329 Selçuk Şener, *Karar Destek ve Üstyönetim Bilişim Sistemleri ve Türkiye'de Bilişim Sektöründe Bir Analiz*, Beykent Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı Yönetim Bilişim Sistemleri Bilim Dalı Yüksek Lisans Tezi, İstanbul, 2006, s. 8, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

de genel sistem anlayışında olduğu gibi daha ötesi kendisi de esasen bir sistem olarak adlandırıldığı için, girdi, çıktı, dönüt ve tüm bunların yer aldığı süreç gibi unsurlara sahiptir.[330] Sonuç olarak bilişim sistemleri ile bilginin toplanması, saklanması, işlenmesi, erişilmesi ve dağıtılmasına hizmet eden teknolojiler (bilgisayar, veri depolama araçları, ağ ve iletişim araçları, yazılım ve geliştirme araçları) uygulama ve hizmetlerin (bilgiişlem, uygulama yazılımı geliştirme, bilgi bankaları ve bilgi erişim hizmetleri vb.) bütünü ve sistem üzerindeki bilgilerin tümü kastedilmektedir.[331]

330 "Bilişim sistemleri organizasyon içerisinde tüm kademelerde bilginin analizi, gösterimi ve sorun çözme gibi konularda karar verme durumundaki kişilere destek sağlamaktadır. Bilişim sisteminin girdisi organizasyon içinden ve çevresinden sağlanan bilgidir. Bu sistemde dönüşüm süreci bilginin islenmesi ve anlamlı hale getirilmesidir. Sonuçta oluşan çıktı ise anlaşılır ve amaca yönelik bilgidir. Bilişim sistemlerinin bilgisayarlarla ilişkilendirilmesi 1990'lı yıllara rastlar. Günümüzde birçok bilişim sistemi yüksek oranda bilgisayar kullanmaktadır. Buna karşın, bir bilişim sisteminin mutlaka bilgisayar kullanması gerekmemektedir. Bilişim sistemleri, organizasyon içinde ve çevresinde önemli insanlar, yerler ve şeyler hakkında bilgi içermektedir. Bilişim denilince insanlar için faydalı ve anlamlı biçime sokulmuş veriler (data) anlaşılmaktadır. Bilişim sisteminde üç aktivite karar verme, işlemlerin kontrolü, problemlerin çözümü ve yeni ürünler veya hizmetler oluşturmada organizasyonların ihtiyacı olan bilgiyi üretmektedir. Bu aktiviteler, girdi (input), çıktı (output) ve işlem (transaction) 'dir. Girdi, organizasyonun içinden veya dış çevresinden, ham bilgileri (veri) ele geçirmek veya toplamaktır. İşlem, bu ham veriyi daha anlamlı bir hale getirmektir. Çıktı ise işlenmiş bilgiyi (information), insanlara veya kullanacak olan aktivitelere aktarır. Bilişim sistemleri aynı zamanda organizasyon içinde seçilmiş olan uygun kişilerin input aşamasını doğrulamasına veya değerlendirmesine yardım eden geri beslemeyi içerir." Bkz. A.e., s. 8-10.

331 D. Arzu Akolaş, "Bilişim Sistemleri ve Bilişim Teknolojisini Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları", *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, ss. 29-43, s. 30, 31, http://dergisosyalbil.selcuk.edu.tr/susbed/article/view/693/645, ET. 27 Ocak 2020.

Şekil 1: Bilişim Sistemi Bileşenleri



Kaynak: J.A. O'Brien, *Indroduction to Information System*, New York, 2001, s.10 (*Aktaran* Özyılmaz, A. F., (2014), *Bilişim Sistemleri, Sağlıkta Bilişim Sistemleri ve Performans*, s. 13)

'Verileri karar vericileri için anlamlı bilgilere çeviren; insan gücü, programlar ve yönetsel süreçlerden oluşan bir set'[332] olarak da ifade edilebilen bir bilişim sisteminin bir bilişim sistemi terimi üzerinde hukuk doktrininde üzerinde fikir birliği oluşan bir tanımı ve hangi unsurlardan oluştuğu konusunda anlaşma bulunmasa da kanaatimizce bir bilişim sisteminin unsurları temel olarak veri, donanım, yazılım ve ağ unsuru olup bu unsurlarının kabulü gereklidir. Zira, verinin girdi, işleme ve çıktı aşamalarını gerçekleştiren sistem[333], ortaya çıkan bilgiyi iletme özelliğini taşımadıkça bir bilişim sistemi olarak kabul edilemeyeceği gibi iletimi sağlayabilecek bir ağ mevcut olsa dahi

332 K. Behan, D. Holmes, Understanding Information Technology, New York, 1990, s. 41 (*Aktaran* Özyılmaz, a.g.e., s. 14).

333 Laudon, bir enformasyon sisteminde girdi, işleme ve çıktı faaliyetlerinin enformasyonu ürettiğini, bilgisayar tabanlı enformasyon sistemlerinin ham veriyi anlamlı enformasyona çevirmek için bilgisayar teknolojisine ihtiyaç duyduğunu fakat bilgisayar ve bilgisayarların bir enformasyon sisteminin sadece bir parçası olduğunu belirtmektedir. Bkz. Kennteh C. Laudon, Jane P. Laudon, *Yönetim Bilişim Sistemleri (Dijital İşletmeyi Yönetme),* s. 16.

veriyi işleyen ve çıktı haline getirmeyi sağlayan donanım ve yazılım unsurları bulunmadıkça bir bilişim sisteminin varlığından söz edilemeyecektir. Söz konusu unsurların tamamı bir bilgisayarda mevcut bulunmakta ise de teknolojinin hız kesmeyen ilerleyişi karşısında bilişim sistemlerinin bugün için bilgisayarlardan ibaret bulunmadığı yadsınamaz bir gerçektir. Günümüzde bilişim sistemlerini en basit hali ile verinin (veya verinin işlenmesi ile oluşan bilginin) bilişim ağları üzerinden bu ağlara bağlanan terminal cihazlar vasıtası düzenlenmesi, depolanmasını, toplanmasını ve iletilmesini sağlayan sistemler olarak ifade edebilmekteyiz. O halde bugünkü anlamıyla tipik bir bilişim sistemi örneği olarak kendi sunucuları (ve sistem odası) bulunan, kullanıcılarının internete çıkabildiği veya bir web sitesi yayınlayabilen bir kurumun bilişim sistemi örnek olarak verebilmekteyiz. Bu sistemin kalbinde sistemin iletişimini sağlayan bilişim ağları yatmaktadır. Veri işleme metodlarında ise hepsinin gerçekleştirmesi gerekmemektedir bu yönü ile doktrinde yer alan "genel amaçlı kullanım" kriteri geçerliliğini ve günümüz şartlarında güncelliğini yitirmektedir. Zira, günümüzde bilgisayarlar birbirinden farklı birçok işi yapabilmesi için tasarlanmaktadır. Nitekim, marketlerde bulunan pos cihazları spesifik bir iş yapması sebebiyle bildiğimiz klasik bilgisayarlara benzememekte ise de içerisinde bilgisayarlarda bulunan CPU, RAM, hafıza alanları ve gömülü bir işletim sistemi bulunan mini bir bilgisayarlardır. Otomatik işleme tabi tutma kriteri ise kavramın belirsizliği adına belirleyici bir kriter olmaktan uzak görünmekte ve söz konusu kriter yerine verinin elektronik başka bir deyişle sayısal veyahut dijital bir ortam üzerinde işlenmesi, depolanması, aktarılması (iletimi) koşulunun dikkate alınması gerektiği düşünülmektedir. Bu bağlamda bankamatikler veya "ATM"[334] leri incelemek gerekirse içerisinde bir para sayma makinesi, fatura kesme makinesi ve üzerinde Windows gibi bir işletim sistemi çalıştıran sıradan bir bilgisayar, evlerimizde bulunan adsl modemler gibi internet servis sağlayıcı sistemine bağlanmayı sağlayan bir modem bulunmaktadır. Esasen para sayma makinesi ve fatura kesme makinesi ATM' nin kendisine bağlı bilgisayarlar olup bankamatikte işlem yapılması ile internet servis sağlayıcısının kiralık hat sistemleri üzerinden bağlanmaktadır. Pos makineleri ise bir

334 "Yargıtay kararlarına yansıdığı üzere, banka ve kredi kartlarının sıklıkla kullanıldığı ATM'ler bilişim sisteminin bir parçası olarak kabul edilmiştir." Bkz. Nusret Onur Akpek, *Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, 2015, s. 82, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.
Yargıtay' ın ATM' lerin bilgileri otomatik işleme tabi tutan sistem olduğunu kabul ettiği karar için bkz. Yargıtay Ceza Genel Kurulu, 10.04.2001, E: 2001/6-30, K: 2001/57.

modem vasıtası ile internete bağlanarak bankanın sistem salonuna sanki bir kullanıcının internete eriştiği gibi erişmekte fakat aradaki bağlantı kriptolu bir tünel vasıtası ile oluşturulmaktadır. Pos makineleri bir bilgisayara benzemese dahi içerisinde bilgisayarlarda bulunan CPU, RAM, hafıza alanları ve gömülü bir işletim sistemi bulunan mini bir bilgisayardır. Bunun yanında el pos cihazlarının da üzerinde bir sim kart bulunmakta ve cep telefonları internete nasıl bağlanıyorsa o şekilde internete bağlanarak merkez sistemlere erişmektedirler. Günümüzde cep telefonlarının mimari açıdan ve çalışma prensipleri açısından incelendiğinde fiziksel bir bilgisayarla aynı unsurları barındırdığı görülmektedir. Hemen hemen günümüzde çoğumuzun fotoğraflarını, belgelerini, şifrelerini, kredi kartlarını ve daha birçok verisini ve hatta tüm yaşamını sakladığı akıllı telefonların kullanımının yaygınlaşması ile bu cihazlar da bilişim suçunun konusunu oluşturmaya başlamıştır.[335] Yargıtay 8. Ceza Dairesi de 2015 yılında vermiş olduğu bir kararda[336] akıllı telefonların kendi işletim sisteminin bulunması doğrultusunda bir bilişim sistemi olarak kabul etmiş ve yerel mahkemenin cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmayacağından bahisle vermiş olduğu kararı bozmuştur. Ancak söz konusu bozma kararında akıllı cep telefonları işletim sistemleri bulunması (yazılım) sebebiyle bir bilişim sistemi olarak kabul edilmişse de bilişim sistemini en basit hali ile verinin (veya verinin işlenmesi ile oluşan bilginin) bilişim ağları üzerinden bu ağlara bağlanan

335 Ömür Uğur, "Pentester Olmak İster Misin?", CyberMag, Sayı: 42, Temmuz 2019, s. 23.

336 "Bilgisayarın çalışmasını düzenleyen tüm programlara işletim sistemi denilmekte olup işletim sistemlerinin sadece bilgisayarlarda değil cep telefonlarında, tablet PC'lerde de kullanılması mümkündür. İşletim sistemleri Windows 8, Android, Linux gibi isimler almaktadır.
Bir bilgisayarın işleyişi ve özellikle de verimliliği, işletim sistemi ile ilgilidir. İşletim sisteminin ana görevi, bilgisayarın çalışması için gerekli komutları vermek ve işlevleri sağlamaktır. Donanım ile yazılım arasındaki bağlantıyı sağlayan işletim sistemi çalışmadığı takdirde bilgisayarın kullanılması, program yüklenmesi olanaksızdır.
….Somut olayda; katılanın cep telefonundan çekilmediği halde sanığın; "Sen Hacer'i değil parayı seviyorsun…., kızım seninle görüşmez, bırak kızımın peşini, dolanma peşinde, seni uyarıyorum, Hacer'in seninle işi olmaz, bir daha bir araya gelmeniz ben hayattayken imkansız" şeklindeki mesajı oluşturduğu ve telefonuna geldiği iddiasıyla boşanma dava dosyasında delil olarak ibraz ettiğinden bahisle açılan davada, sanık suçlamayı kabul etmemiş, bilirkişi raporunda ise iletişim detaylarında suça konu mesajlaşmaya dair kayıt bulunmadığı, ancak cep telefonlarına özel yazılımlar yüklenerek veya internet vasıtasıyla mesaj oluşturulabileceği belirtilerek mesaj çekilen ve mesaj alan cep telefonlarının incelenip, iletişim kayıtlarıyla karşılaştırılması gerektiğinin bildirilmesi karşısında, cep telefonlarında mobil işletim sistemleri bulunduğu ve program yüklenebilmesinin mümkün olduğu gözetilerek, taraflara ait cep telefonları alınıp uzman bilirkişi tarafından incelenip, iletişim kayıtları ile karşılaştırılmak suretiyle program yükleme veya internetten gönderme şeklinde suça konu mesaj gönderilip gönderilmediğinin araştırılması, sonucuna göre sanığın hukuki durumunun tayin ve takdiri gerekirken, cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmayacağından bahisle, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, Yasaya aykırı, (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 18.3.2015 t., E: 2014/30037, K: 2015/14023, www.kazanci.com›kho2/ibb/giris.html, ET. 13 Temmuz 2020.

terminal cihazlar vasıtası düzenlenmesi, depolanmasını, toplanmasını ve iletilmesini sağlayan sistemler olarak ifade ettiğimizden başka bir deyişle bir bilişim sisteminin aynı zamanda ağlar aracılığıyla verinin iletimi (aktarımı) unsurunu da içermesi gerektiğinden mezkur Yargıtay kararının gerekçesinin doğru olmakla birlikte eksik olduğunu belirtmek isteriz.[337]

Bugün için içerisinde bulunduğumuz başta üretim olmak üzere birçok alanda Bilgi İletişim Teknolojilerinin sunduğu dijital teknolojilerden yararlanarak dijital altyapı oluşturulması yaklaşımını başka bir deyişle entegrasyon sürecini ifade eden "dördüncü sanayi devrimi (endüstri 4.0.)"[338] için gereken teknolojiler nesnelerin interneti (IoT- Internet of Things), akıllı robotlar, akıllı sistemler, simülasyon, siber güvenlik, sanal gerçeklik, bulut teknolojisi, eklemeli üretim, artırılmış gerçeklik, büyük veri, 3D, mobil cihaz teknolojileri, blok zinciri teknolojisi (blockchain), haberleşme teknolojileri gibi)[339] sayesinde bilişim sistemi olarak kabul edilebilecek yeni sistem, cihaz ve aygıtlar hayatımıza girmiş ve girmeye devam etmektedir. Nesnelerin internete bağlanarak diğer nesnelerle haberleşmesi olarak ifade edilmekte olan IoT (Internet of Things) kavramı, çeşitli protokoller sayesinde birbirlerine bağlanarak bulut üzerinden bilgiyi paylaşıp işleyen akıllı cihazlar arasında gerçekleşmekte olup akıllı şehirler, akıllı çevre, lojistik, sağlık uygulamaları, araç takip sistemleri, hasta takip sistemleri, otomotiv ve ulaşım uygulamaları, endüstriyel uygulamalar, savunma sanayi gibi birçok uygulama alanı bulunmaktadır.[340] IoT'de

337 Aynı yönde bkz. Karagöz, a.g.e., s. 38.
338 Gerçek ve Gökşen, a.g.e., s. 25.
339 Ayrıntılı bilgi için bkz. a.e., s. 27-56.
340 "Örnek IoT Cihazları
Nest- Google tarafından satın alınan bu ürün evde olmadığınız zamanlarda uygulama üzerinden evin sıcaklığını kontrol etmemizi sağlıyor.
Hapifork- Hapifork fazla ve hızlı yeme durumlarında uyararak düzenli beslenme alışkanlığı sağlayan akıllı bir çataldır.
Micoach akıllı top- Adidas'ın çıkardığı bu top atılan penaltıların kaç gol olduğunu, hangi ayakla atıldığını ve kaç km öteden atıldığını gösteriyor.
Smart Things- Akıllı evler için yapılan bir IoT cihazıdır. Ürünü akıllı telefonda kullanabileceğiniz uygulamayla entegre ederek çalıştırabilirsiniz. Bu akıllı cihaz ile sabah uyandığınızda kahveniz hazırlanabilir ya da eve geldiğinizde ışık ve müzik sistemi otomatik açılabilir.
Babolat- Babolla akıllı bir raket cihazıdır. Tenisçilerin topa vuruş hızlarını, vuruş açılarını, hangi elle ve stille vurduklarını uygulamayı cihazla entegre ederek gösterilebilen bir akıllı cihazdır.
Edyn- Edyn toprağa ne ekmeniz, nasıl ekmeniz ve toprağı hangi aralıklarla sulamanız gerektiği konusunda önerilerde bulunuyor.
Amazon Echo- Söylenilen komutları yerine getirip dahili hoparlöründen cevapları ileten akıllı bir hoparlör cihazıdır. Akıllı cihazlarda kullanılabilen uygulama ile entegre edilerek çalıştırılabilne bir cihazdır.
Bluesmart- Dünyanın ilk akıllı valizidir. İçerisinde digital kilit ve mesafe algılayıcısı bulunan cihaz siz uzaklaşınca kendini otomatikman kilitliyor. Dahili tartısıyla valizin ağırlığı ölçülebiliyor, konum takibi yapabiliyor ve dahili şarj aletiyle telefonunuzu şarj edebilirsiniz." Bkz. İSTANBUL TEKNİK

kullanılan akıllı algılayıcı cihazlar kendilerini tanıtma, ağ kurabilme ve topladıkları bilgileri depolama ve analiz yeteneğine sahip genel kullanıma açık bulut servislerine aktarma yeteneğine sahip olup kullanıcıların bu servislere ulaşımı ve istedikleri analiz sonuçlarını alabilmeleri kolay kullanımlı web servisleri aracılığıyla gerçekleştirilmektedir.[341] 2017 yılında nesnelerin interneti üzerinde yapılan ilk siber saldırıdan sonra konuya verilen önem artmış siber uzayı daha da genişleteceği, nesnelerin interneti ile yapılacak saldırıların çeşitlilik kazanacağı belirtilmekte ve bu ağların büyümesi de göz önüne alındığında bu konuda da çalışmalar yapılması gerektiği vurgulanmaktadır.[342] Bir bilgisayarın veya bilgisayar kontrolündeki bir robotun çeşitli faaliyetleri zeki canlılara benzer şekilde yerine getirme kabiliyeti olarak tanımlanabilen, makine öğrenmesi, yapay sinir ağları, derin öğrenme, görüntü tanıma, doğal dil işleme gibi birçok alt alanı içeren ve yeni yüzyılın en önemli teknolojilerinden biri olan yapay zeka teknolojisi, büyük miktarda veriyi hızlı, tekrar eden işlemler ve akıllı algoritmalar ile birleştirerek yazılımın kalıplarından veya özelliklerinden otomatik olarak öğrenmesini sağlamak üzere kurulmuş olup otonom araçlardan robotlara, eğlence dünyasından bankacılığa, sağlık ve sigorta şirketlerinde vb. farklı birçok uygulama alanında yer edinmiştir.[343] Bu yönü ile yapay zekâlı aygıtların bilişim sistemi unsurlarını taşıdığı tereddütsüz kabul edilebilecektir. Yine dijital dönüşüm çağında artan veri miktarı ile yüksek kapasiteli veri depolama alanlarına ihtiyaç duyulmasının neticesinde ortaya çıkan veri analizinin yapılabildiği, üzerinde herhangi bir yazılım veya aracı kullanılabildiği, siber ataklara karşı önlemlerin alındığı bir bağlantı yapısıyla sürekli bağlantının gerçekleştirilebildiği bilgi teknolojileri altyapısından hizmet almak anlamına da gelen bulut teknolojisi[344] ile esasen fiziki olarak kurulmuş bir altyapıdan yararlanılıyormuş gibi kullanılabilen bulut sistemler[345] de bir bilişim sistemine başka bir örnek oluşturmaktadır.

Sonuç olarak, 5237 sayılı TCK' nın 243. m.' sinde "bilişim sistemi" kavramının benimsenmiş olması, hızla gelişen ve yaşamımızın neredeyse her alanına

ÜNİVERSİTESİ, "Internet of Thing (IOT)", 15.01.2019, https://bidb.itu.edu.tr/seyir-defteri/blog/2019/01/15/internet-of-thing-(iot), ET. 01 Şubat 2020.

341 Ercan ve Kutay, a.g.e., s. 600.

342 Sağıroğlu, a.g.e., s. 48.

343 Gerçek ve Gökşen, a.g.e., s. 53.

344 A.e., s. 41.

345 "Bulut ortamlar, kullanıcıların hizmetlerini uzaktan ama belirli bir merkez yapı içerisinden almalarını sağlayan, kullanımı kolay uygulamalar ve hizmetler sunan, kişisel bilgiler ve dosyaların güvende olduğundan emin olunan fakat sunduğu fırsatlar kadar da bünyesinde güvenlik riskleri barındıran yapılardır." Bkz. Sağıroğlu, a.g.e., s. 52.

nüfuz eden teknolojik gelişmeler karşısında kapsayıcı bir terim olması açısından doğru bir yaklaşımdır. Bununla birlikte 243. m.' nin gerekçesinde yer alan "verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma imkanı veren manyetik sistemler" tanımının "bilişim sistemi" kavramını açıklamada yeterli olmadığı görülmektedir. Öncelikle belirtmek gerekir ki, çok hızlı değişen, gelişen ve sınırları belli olmayan bilişim alanına ilişkin statik ve sınırları daraltıcı nitelikte tanımlama çalışmalarının doğru sonuçlar doğurmayacağı bir gerçek olmakla birlikte kanunilik ve belirlilik ilkelerinin geçerli olduğu ceza hukukunda bu suç tiplerine ilişkin kendilerine özgü yapıları dikkate alınmak suretiyle en azından muğlak olmayan kapsayıcı belirlemelerin yapılması gereği de göz ardı edilmemelidir. Gelişen teknoloji ile birlikte ortaya çıkan yeni sistemlerin varlığı[346], (akıllı telefonlar, tabletler, akıllı cihazlar vb.) bilişim suçlarının günümüzde sadece bilgisayarlarla değil bilişim temelli bu cihazlarla da işlenilebilmesi[347], 5237 sayılı TCK' nın 243. m.' sinin gerekçesinde yer alan bilişim sistemi kavramının tanımının güncellenmesini kaçınılmaz hale getirmektedir. Zira, günümüzde yeni dijital ve akıllı üretim teknolojileri ile ortaya çıkan "nesnelerin interneti" sağlıktan, endüstriye, ulaşım ve kamu hizmetlerinden, bina ve ev otomasyonuna kadar etki alanı yaratacak iken bir bilişim sisteminin, sadece verileri toplayıp yerleştirme sonrasında bunları otomatik işleme tabi tutabilme özelliklerini içereceğinin kabulü günümüz teknolojisine ve koşullarına uymamaktadır. Bu bağlamda, bir bilişim sisteminin söz konusu unsurların yanı sıra veriyi gönderebilme (iletebilme/aktarabilme) özelliğini de ihtiva ettiği gerçeğinin gerekçede yer alan tanıma eklenmesi doğru bir yaklaşım oluşturacaktır. Diğer taraftan, gerekçede yer alan tanımda "manyetik sistem" ifadesinin, bilişim sistemlerini ifade etmede yanlış bir ifade oluşturmadığı değerlendirilse de bir bilişim sistemini tanımlamada belirleyici bir unsur niteliği taşımadığı ve mevcut tanımdan çıkartılmasının da uygun olacağı düşünülmektedir.

346 Dülger' e göre bilgisayarlar bilişim sistemine dahil olmakla birlikte uygulamada cep telefonları, kişi ile araçları tanıyan otomatik sistemler, araç bilgisayarları kavramları da bilgisayar sistemi kavramı içerisine girmektedir, bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 61.

347 Onur Sarı, *Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar*, Harp Akademileri Stratejik Araştırmalar Enstitüsü Harp/Harekat Hukuku Ana Bilim Dalı Yüksek Lisans Tezi, İstanbul, 2013, s. 75, https://tez.yok.gov.tr/UlusalTezMerkezi/, 13 Temmuz 2020.

1.2. BİLİŞİM SUÇLARINA İLİŞKİN GENEL BİLGİLER

1.2.1. Bilişim Suçu Terimi ve Doktrinde Yer Alan Diğer Terimlerle Karşılaştırılması

Bilişim suçu kavramı, bilişim teknolojilerinin ortaya çıkması ile ceza hukukunda tartışılmaya başlanılan, kendisine özgü nitelikleri olan, henüz üzerinde uzlaşmanın sağlanamadığı bir kavram[348] olup "bu kavramı ifade etmek için "bilgisayar suçu"[349], "siber suç"[350], "internet suçu"[351], "bilgisayar ile ilgili suç"[352], "ileri teknoloji suçu"[353], "bilgisayar ağları kullanılarak işlenen suçlar"[354], "sanal suç" gibi birçok farklı terim de kullanılmıştır. Doktrinde, gelişen teknoloji karşısında bilişim suçlarına çerçeve çizmenin zor olduğu bu sebeple bu suçlara "çizgisiz çerçeveli suç" da denildiği belirtilmektedir.[355] Henüz gerçek anlamda bu alanın tamamını kapsar nitelikte açıklayıcı bir terim haline gelen bir terim mevcut bulunmayıp bu terimlerin çoğu birbirlerinin alternatifi olarak kullanılmaktadır.[356] Hangi terimle ifade edilirse edilsin

348 Cengiz Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", *Ceza Hukuk Dergisi*, Yıl: 10, Sayı: 29, Aralık 2015, ss. 205-263, s. 207; Cengiz Apaydın, "Bilişim Sistemine Girme Suçu", *Türkiye Adalet Akademisi Dergisi*, Yıl: 7, Sayı: 24, Ocak 2016, ss. 245- 306, s. 248; Servet Yetim, "Bilişim Suçları ve Etkin Mücadele Yöntemleri", *Terazi Aylık Hukuk Dergisi*, Cilt: 9, Sayı: 95, Temmuz 2014, ss. 80- 86, s. 81.

349 Recep Yılmaz Yazıcıoğlu, *Bilgisayar Suçları : Krimonolojik, Sosyolojik ve Hukuki Boyutları İle*, Alfa Yayınları, İstanbul, 1997.

"Yazıcıoğlu' na göre, bilişim araçlarının en yaygın olanı bilgisayar olduğundan ve "bilgisayar suçları" teriminin kullanılması alışkanlık haline geldiğinden, genelde "bilişim alanındaki suçları" tarif etmek için "bilgisayar suçları terimi kullanılmaktadır…Dolayısıyla "bilişim alanındaki suçlar" denilince bilgisayarları da kapsayan ve özellikle bilgisayar ve bu tür aygıtların yer aldığı bir alanı ifade ettiği belirtilmektedir." Bkz. Doğan, a.g.e., s. 15.

350 İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye' de Durum*, 1. Bsk., Adalet Yayınevi, Ankara, 2008; İlker Kara ve Gamze Kaya, "Türkiye' de Bilişim Alanında İşlenen Suçların Uygulama Bakımından Hukuki Boyutunun Değerlendirilmesi", *Kazancı Hukuk Araştırmaları Dergisi*, ss. 154- 167, s. 155.

351 Cevat Özel, "Bilişim-İnternet Suçları", https://docplayer.biz.tr/583371-Bilisim-internet-suclari.html, ET. 02 Kasım 2019.

352 Hasan Dursun, "Bilgisayar İle İlgili Suçlar", *Yargıtay Dergisi*, Sayı: 1-2, Ocak-Nisan 1998, ss. 334-339.

353 "Son zamanlarda, "cybercrime" kavramına eş anlamlı olarak "hi-tech crime" yani "yüksek teknoloji suçu" ve "e-crime" kavramları da kullanılmaktadır…Bilişim suçları, özellikle dünya çapındaki internet ağı nedeniyle bu şekilde ifade edilmiştir." Bkz. Karagülmez, a.g.e., s. 43; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 208, dipnot: 14.

Akbulut, ileri teknoloji kavramını daha ileri teknolojilerin her zaman hayatımıza girebileceği, dolayısıyla söz konusu suçların hepsinin bu nitelikte olmayacağı düşüncesi ile kabul etmediğini belirtmektedir. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 59.

354 Özen ve Baştürk, a.g.e., s. 89.

355 Doğan, a.g.e., s. 43.

356 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 147.

Yine Dülger' e göre, sözkonusu terimlerin sözcük anlamı ile yaklaşılması halinde her bir terim içerisinde bir veya daha çok eksikliği barındırabilecek olup bu terimler suçun işlenmesinde teknolojinin rolünü vurgulayan geniş çerçeveli betimleyici terimler olduğundan sözcük anlamları ile yaklaşılmamalıdır. Bkz. Dülger, a.e.

şu bir gerçektir ki, "bu suçlarının işlenme yeri; bilgisayar ve yan teknolojilerinin birbirleri ile bağlantıları ve haberleşmeleri sırasında oluşturdukları sanal alan ve bu sistemlerin çalıştığı network sistemleridir"[357]. Biz de terimleri ayrıntılı incelemeye geçmeden önce, çalışmamız içerisinde ilgili kaynağında belirtildiği şekilde kullanılacak olan terimlerin hepsinin esasen bilişim suçu terimi yerine kullanıldığını belirtmek isteriz.

Bilişim suçlarının 1960' lı yıllardan itibaren Amerika' da ortaya çıkması sonucunda Amerikan doktrininde çoğunlukla kullanılan "computer crimes" (bilgisayar suçları) terimi[358] Amerikan hukukunda 'bilgisayar verilerinin çalınması ya da sabote edilmesi veya herhangi bir suçun işlenmesi için bilgisayarın kullanılması gibi bilgisayar teknolojisini gerektiren suç çeşidi'[359] olarak açıklanmaktadır. Öncelikle belirtmek gerekir ki her ne kadar bilişim suçlarının anavatanı olarak nitelendirilebilecek ABD hukukunda "bilgisayar suçu" terimi kullanılmakta ve kabul görmekte ise de yapılan tanıma bakıldığında bu terimin bir cihaz olarak sadece bilgisayarı içeren değil bilgisayar teknolojisini gerektiren bir suç olduğunun altı çizilmiştir.

Türk doktrininde ise, "bilişim suçu" ve "bilgisayar suçu" terimleri arasında anlam ve kapsam farklılığı yaratılmakta, bu farklılık da esasen bilişim suçlarında suçun konusunu oluşturan veya suçta araç olarak kullanılan "bilgisayar" ve "bilişim sistemi" nin kapsamını belirlemeye ilişkin üzerinde görüş birliği oluşturulamamış tartışmalardan kaynaklanmaktadır.[360] Halbuki "bilgisayar suçu", "bilişim suçu" gibi terimler, bu terimler altında işlenecek suçların hukuki konuları açısından kategorik bir nitelik taşımamaktadır.[361] O halde, bu noktada inceleme konumuz doktrinde kullanılmakta olan farklı birçok terim ve adlandırmadan hangisinin bu suç tiplerinin tamamını kapsayan ve doğru ifade eden bir nitelik taşıdığını belirlemek ve buna uygun bir terim seçmek olmalıdır. Bu bağlamda, doktrinde "bilgisayar suçu" terimi de haklı

357 Yetim, a.g.e., s. 81.
358 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 46.
359 Black's Law Dictionary, Ed: Bryan A. Garner, Seventh Edition, St. Paul Minn, West Group, 1999, s. 392 (*Aktaran* Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 72).
360 Zira, doktrinde yer alan tanımlara bakıldığında, "bilişim suçu", "bilgisayar suçu" terimleri arasındaki tanım farklılıkları, bilgisayar ve bilişim sistemi terimlerinin arasındaki anlam ve kapsam belirlenmek suretiyle aralarındaki farklar esas alınarak yapılmaktadır. Bkz. Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları,* s. 34, 35.
361 A.e., s. 38.

olarak eleştirilmiştir.[362] Bu eleştiriler, bilişim suçlarının sadece bilgisayarlarla işlenmemesi, bu bağlamda gelişen teknoloji karşısında kavram yetersizliğinin yaşanabileceği üzerinde yoğunlaşmıştır.[363] Bunun yanında bilgisayarın tek başına suç işleyemeyeceği bu terimle kast edilenin bilgisayar aracılığı ile işlenebilen suç olduğu ancak bilgisayar aracılığıyla işlenen bir suça bilgisayar suçu denilmesinin anlamsız olduğu da getirilen eleştiriler arasındadır.[364] Nitekim, Erdoğan da kullanılan diğer tüm terimleri kastederek suçlara kullanıldığı araca göre isim verilemeyecek olunması nedeniyle bu terim ve kavramların yetersiz kaldığını belirterek "bilişim suçu" terimini benimsemektedir.[365] Değirmenci ise, bilişim sistemlerinin en yaygın olanının bilgisayarlar olması nedeniyle "bilgisayar suçları" kavramının "bilişim suçları veya suçluluğu" terimi ile hatalı olarak eş anlamda kullanıldığını belirtmektedir.[366] Ersoy ise, bilişim suçundan bilgisayarı da kapsayan ancak daha geniş olan bilişim araçlarına karşı veya onlar aracılığı ile işlenen suçları anlamak gerekmekte olup bilişim

362 Kurt, ABD' de bilgisayar suçları ile ilgili ilk düzenlemelerin yapıldığı sıralarda internet ve iletişimin günümüzde olduğu kadar yaygın olmaması sebebiyle "bilgisayar suçu", "bilişim suçu" terimlerinin tanımları arasında birbiriyle benzerlikler bulunduğunu, bu ülkenin mevzuatından etkilenen akademik çevreler ve diğer ülke mevzuatlarında da bu terimlerin birbiri yerine kullanıldığını belirtmektedir. Bkz. Kurt, a.g.e., s. 52.
Değirmenci, " "Bilgisayar suçları" terimi hatalı olarak "bilişim suçları ve suçluluğu" terimi ile aynı anlamda kullanılmaktadır. Bu terimle, içinde en az bir bilgisayar olan bilişim sistemlerine karşı veya bu sistemler ile işlenen suçlar kastedilmektedir. Bu çalışmada, hem Türk Ceza Kanunumuzun "bilişim alanında suçlar" terimini tercih etmesinden, hem de "bilgisayar suçları" kavramının, "bilişim suçları" kavramını tam olarak ifade edememesinden dolayı "bilişim suçları" terimini genel olarak kullanmakla birlikte, yer yer "bilgisayar suçları" terimine de eş anlamda olmak üzere yer vereceğiz." hususlarını belirtmiştir. Bkz. Değirmenci, "Bilişim Suçları", s. 55.
363 Bkz. Taşkın, a.g.e., s. 12; Akbulut, *Bilişim Alanında Suçlar*, s. 59.
Taşkın' a göre: "Öyleyse, gelişen teknoloji karşısında, bilişim suçlarının gösterdiği gelişmede yasaların yetersiz kalabilme olasılığını ortadan kaldırmak için, bilişim sistemlerine karşı işlenen suçlara (ya da bu sistemlerin araç olarak kullanılması suretiyle işlenen suçlara) yeni bir kavram bulunması, hızlı gelişen bilişim teknolojisi karşısında yasaların yetersiz kalma tehlikesinin bir ölçüde önüne geçebilecektir…Aksi halde, bugünkü teknolojinin ulaştığı noktada, örneğin bir cep telefonu ile işlenen ya da ileride akıllı evler aracılığıyla işlenebilecek olan bilişim suçlarının cezasız kalması tehlikesi belirebilecektir. Bu durumda, cep telefonunu veya başka amaçlı elektronik cihazları "bilgisayar" sözcüğünün içerisine hapsetmek doğru değildir." Bkz. Taşkın, a.g.e., s. 11, 12.
Kurt' a göre: "Bilişim alanının bir unsuru olarak kabul ettiğimiz internette işlenen ve bilgisayar suçu tanımı içine girmeyen suçlar bulunmaktadır. Verilerin işlenmesi ile ilgili olmayıp iletilmesi ile ilgili olan bu suçların tamamının bilgisayar suçu terimi ile karşılanması mümkün değildir. Bilişim alanında bilgisayar suçlarının dışında da suçların işlenmesi mümkündür. Üst kavram olarak öngördüğümüz bilişim alanında bilgisayar suçu işlenebilecek suç kategorilerinden sadece bir tanesidir." Bkz. Kurt, a.g.e., s. 52.
Pallı' ya göre: "bilişim alanında işlenen suçlar, bilgisayar ile kısıtlı olmayıp bunun yanında bu alandaki başkaca cihazlar vasıtasıyla veya onlara karsı islenmesi durumunda da söz konu olacaktır. Burada öne çıkan "bilisim alanında suçlar" kavramının 765 sayılı TCK'da kullanılma sebebinin de bilişim suçlarını bilgisayarla sınırlandırmamak olduğu anlaşılmaktadır." Bkz. Pallı, a.g.e., s. 43.
364 Değirmenci, "Bilişim Suçları", s. 55.
365 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, s. 47.
366 Değirmenci, "Bilişim Suçları", s. 54.

araçlarının en yaygın olanının bilgisayarlar olması ve diğer bilişim araçlarının da bilgisayar esasına dayanması sebebiyle bilgisayar suçu kavramının da kullanıldığını belirtmektedir.[367]

Kurt' a göre ise, bilişim alanında işlenen suçların tamamı bilgisayar suçları olmayıp farklılık gösteren türleri bulunmakta olup ağ ya da internet üzerinden işlenen veya siber suç özelliği gösteren eylemlerin oluşturduğu farklı kategorideki bu suçların tamamı bilişim suçu üst başlığı altında toplanmaktadır.[368]

Diğer taraftan, "internet suçu" terimi ise sadece ağları esas alması nedeniyle başka bir deyişle bu suçların sadece ağlar aracılığıyla işlenmemesi[369], ayrıca internet kullanımı en yaygın ağ olsa da bunun dışında intranet, ekstranet gibi başka ağların da varlığı karşısında bilişim suçlarının bu diğer ağlarla da işlenmesinin mümkün olması sebepleriyle[370] haklı olarak eleştirilmiştir. Zira, bilişim suçları sadece internet üzerinden değil bilginin teknoloji ile iletildiği her alanda işlenebildiği, cep telefonu ve kredi kartlarının bunlara örnek olduğu belirtilmiştir.[371]

Uluslararası literatürde daha yoğun kullanılan[372] "siber suç"[373] terimi ise bilişim suçlarını ifade etmede kullanılan bir diğer terim olup "internet suçu" teriminde olduğu gibi ağ sistemlerinden yola çıkılarak kullanılan[374], esasen internet dışındaki diğer bilişim ağlarını da kapsayan bir üst kavram olan "siber uzay"[375] dan yola

---

367 Ersoy, a.g.e., s. 151.
368 Kurt, a.g.e., s. 143.
369 Akbulut, *Bilişim Alanında Suçlar*, s. 59.
370 Yılmaz Yazıcıoğlu, *"Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı"*, Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001, İzmir, Dokuz Eylül Üniversitesi Yayını, 2002, ss. 451-470, s. 452, dipnot:3; Yener Ünver, "Türk Ceza Kanunu' nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, C.LIX, S. 1-2, İstanbul, 2001, ss. 51-153, s. 79; Yenidünya ve Değirmenci, a.g.e., s. 31, 32 (*Aktaran* Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 74); Taşkın, a.g.e., s. 11.
371 Orta, *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim),* s. 87.
372 Rezan Epözdemir, "Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri", *Terazi Aylık Hukuk Dergisi*, Bilişim Hukuku Özel Sayısı, Cilt: 13, Sayı: 142, Haziran 2018, ss. 88-98, s. 89.
373 "Siber suç, bilgisayar ve ağ sistemleri yoluyla bilgisayar veya ağ sistemleri içerisinde ya da bilgisayar tarafından suç olarak yaratılmış fiillerin siber ortamda işlenmesi ve daha önce suç olarak yaratılmamış bu ortamın karakteristiğine has bir takım ihmallerin bütünüdür." Bkz. Demircan, a.g.e., s. 22.
374 Akbulut, *Bilişim Alanında Suçlar*, s. 57.
375 Siber uzay, İngilizce-Türkçe Ansiklopedik Bilişim Sözlüğü' nde: "cyberspace: siber uzay. Bilgisayarlar, bilgisayar ağları ve kullanıcılarının oluşturduğu sanal topluluk." olarak tanımlanmıştır. Bkz. *İngilizce-Türkçe Ansiklopedik Bilişim Sözlüğü*, s. 177.
"Siber uzay", doktrinde ise, "işlemci ve kontrolörlerin bulunduğu internet, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarının olduğu küresel bir alan" şeklinde tanımlanmaktadır. Bkz. Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 54.

çıkılarak tercih edildiği görülen bir terimdir.[376] Başka bir anlatımla, "siber suç"[377], tek bir bilişim sisteminde değil, bilişim sistem ağları vasıtasıyla özellikle de internet aracılığıyla gerçekleştirilen eylemleri ifade etmek üzere kullanılan bir terimdir.[378] Artuk-Gökçen-Yenidünya' ya göre, "bilişim suçları", "siber suçlar" kavramına göre üst bir kavramdır ve "siber suçları" da içine alır.[379] Avustralyalı hukukçu Clough "siber suç" terimini kullanmasının sebebini öğretide ve edebiyatta yaygın olarak kullanılması ve bu terimin ağa bağlı bilgisayarların önemini vurgulaması olarak belirtmiştir.[380] Avrupa Konseyi Siber Suç Sözleşmesi, "siber suç" terimi kullanımı tercih edilmiş[381] ancak siber suçu tanımlamamış bunun yerine suçları sayma suretiyle belirleme yolunu tercih etmiştir.[382] UNODC Siber suçların ve siber saldırıların uluslararası bir tanımı bulunmadığını belirterek suçların genellikle bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar, bilgisayarla ilgili suçlar, içerikle ilgili suçlar ve telif hakkı ve ilgili hakların ihlali ile ilgili suçlar kategorileri etrafında kümelendiğini belirtmektedir.[383] Interpol ise resmi

376 Eker, a.g.e., s. 104.

377 'bilgisayar veya ağ sistemleri yolu ile bilgisayar veya ağ sistemleri içerisinde ya da bilgisayar ve ağ sistemlerine karşı işlenebilir.' Bkz. Hans Corell, "The Challenge of Borderless Cyber-Crime", 14 Aralık 2000, Syposium On The Occassion of The United Nations Convention Against Transnational Organized Crime, Palermo, http://www.unodc.org/palermo/corell1.doc Erişim Tarihi:27 Mart 2008 (*Aktaran* Haydar Çakmak, Cenker Korhan Demir, Suç, Terör & Savaş Üçgeninde Siber Dünya, "Siber Dünyadaki Tehdit ve Kavramlar", Ed.: Haydar Çakmak, Taner Altunok, Ankara, Barış Platin Kitabevi, 2009, s. 34, ss. 23-55).

378 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 45.

Erdoğan' a göre, "bilişim suçları" kavramı, "siber suç" kavramına göre üst bir kavram olup "siber suçlar" ı da içine almaktadır. Bkz. A.e.

379 "Bu kavram da esasen bilişim alanında işlenen suçları ifade etmektedir. Ancak, siber suç; tek bir bilişim sisteminde değil, bilişim sistem ağları vasıtasıyla (özellikle internet) gerçekleştirilen eylemleri ifade etmek üzere kullanılmaktadır. Konuyla ilgili bir tanımda siber suç "bilgisayarların amaç veya araç veya her ikisi olarak kullanıldığı hukuka aykırı eylem" şeklinde ifade edilmiştir." Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6890.

Yaşar, Gökcan, Artuç' a göre de: "YTCK'nın 243. maddesi metninde, bilgisayar suçları veya internet ile ilgili suçlar yerine "Bilişim Suçları" tabirinin kullanılması yerinde olmuştur…Yine bu tabir, tek bir bilişim sisteminde değil, internet gibi bilişim sistemi ağları vasıtasıyla gerçekleştirilen eylemleri kapsayan "siber suç" tabirine göre daha üst bir kavramı ifade ettiğinden, anılan terime göre de daha yerinde bir kavramdır." Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7286.

380 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 147.

381 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 45.

382 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* s. 51.

383 Genel olarak, siber suçlar siber bağımlı suçlar, siber etkin suçlar ve belirli bir suç tipi olarak, çevrimiçi çocuk cinsel sömürüsü ve istismarı olarak tanımlanabileceği, siber bağımlı suçun bir BİT altyapısı gerektirdiği ve genellikle kötü amaçlı yazılımların, fidye yazılımlarının, kritik ulusal altyapıya yönelik saldırıların oluşturulması, yayılması ve dağıtılması (örn. bir enerji santralinin organize suç örgütü tarafından siber olarak devralınması) ve bir web sitesini veri (DDOS saldırısı) ile aşırı yükleyerek çevrimdışı hale almak olarak gerçekleştirileceği, siber etkin suç çevrimdışı

sitesinde "Siber suç" için "Saf siber suç" bilgisayarlara ve bilgi sistemlerine karşı işlenen suçları ifade ettiğini; burada amacın bir cihaza yetkisiz erişim sağlamak veya yasal bir kullanıcıya erişimi reddetmek olduğunu bunun yanında "siber özellikli" suçların, hırsızlık, dolandırıcılık, yasadışı kumar, sahte ilaçların satışı gibi yeni olmak zorunda olmadığını ancak yeni bir çevrimiçi boyut kazandığını belirtmektedir."[384] İngiliz hukukçu Walden ise "siber suçlar" kavramının "bilgisayar suçlarının" alt kümesi olduğunu ancak yine de bu iki terimin eş anlamlı olarak kullanıldığını belirtmektedir.[385] Türk doktrininde de kullanılan bu terimin bilişim suçlarını tam olarak karşılayan bir terimi oluşturmadığını düşünmekteyiz. Zira, Erdoğan' ın da belirtmiş olduğu gibi, Sözleşme' nin uygun bulunması için hazırlanan Kanun' da "siber" kavramına karşılık olarak "sanal" kelimesi tercih edilmişse de "siber"[386] kelimesi TDK tarafından tanımlanmamış olup bunun yanında söz konusu suçların neticeleri somut dünyada gerçekleştiğinden yani bu suçların neticeleri "sanal" olmadığından bu terimin kullanılması yerinde bir tercih olmayacaktır.[387] Kaldı ki, bilişim suçları sadece ağlar aracılığı ile işlenmediğinden bu terim de, kavramı ifade etmekte yetersiz kalacaktır. Her ne kadar Türkçe' de "siber" kavramının karşılığı olarak "bilişim" kelimesi kullanılmakta ve zaman zaman birbirleri yerine kullanılmakta ise de çok belirgin olmamakla birlikte "siber" kavramından bilgisayar ve buna bağlı elektronik sistemlerin bulunduğu ortam, "bilişim" ile de bu ortamdan etkin olarak faydalanma ve bu ortam aracılığı ile bilgi üretilmesi şeklinde anlamların çıkarılabilmesi mümkün olup "bilişim" kavramının "siber" kavramının ötesinde bir anlamı işaret ettiğini söyleyebilmekteyiz.[388]

---

dünyada oluşabilmesi ama aynı zamanda BİT tarafından kolaylaştırılabilir olması olarak belirtilmekte olup genellikle çevrimiçi dolandırıcılık, çevrimiçi uyuşturucu alımları ve çevrimiçi kara para aklamayı içermektedir. Bkz. UNODC, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

384 Bkz. INTERPOL, https://www.interpol.int/Crimes/Cybercrime, ET. 1 Mart 2020.

385 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 147.

Dülger ise bu görüşe katılmamakta ve "bilgisayar suçları" kavramının "siber suçlar" kavramının alt kümesini oluşturduğunu düşünmektedir. Bkz. A.e.

386 Siber kelimesi "sibernetik" sözcüğünün kısaltılması olarak kullanılmakta olup üzerinde fikirbirliği bulunan bir anlamı mevcut olmasa da "süreçleri ve iletişimi kontrol etme ve yönetme, bilgisayar ve internetle ilgili" anlamını işaret ettiği belirtilmektedir. Bkz. Çakmak ve Demir, a.g.e., s. 25, 26.

387 A.e., s. 50. Benzer yönde görüş için bkz. Ünver, a.g.e., s. 79; Yazıcıoğlu, *"Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı"*, s. 452, dipnot:3 (*Aktaran* Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 74)

388 Çakmak ve Demir, a.g.e., s. 26.

İngiliz hukukçu Gillespie: 'Herhangi bir bilgisayar siber alana bağlı olmak ihtiyacında değildir (bizim konumuz açısından internete), dolayısıyla bir internet suçuyla ilgileniyorsak, bazı bilgisayar

Kanaatimizce, Türk Ceza Kanunu' nda yer alan "Bilişim Alanında Suçlar" başlığının tercih edilmesinin[389] ve bu başlık altında yer alan suç tiplerinde kullanılan terim ve terminolojinin, gelişen teknoloji karşısında kapsayıcı olabilmesi amacını güttüğü ve bu doğrultuda suç tiplerini ifade etmekte "bilişim suçu" teriminin tercih edilmesinin Ceza Kanunu' muzla terminoloji bakımından da uyumlu olması açısından daha doğru olacağı[390] düşünülmektedir. Kaldı ki ülkemizde de 2000' li yılların başından itibaren yasal düzenlemelerde ve doktrinde genel olarak "bilişim suçu" terimi üzerinde uzlaşma sağlandığı söylenebilmektedir.[391] Ancak çalışmamız içerisinde ilgili bölümlerde ve özellikle de yabancı kaynaklardan alıntılanan yerlerde "siber suç" terimi kullanılmış olup bununla kast edilenin kabul etmekte olduğumuz "bilişim suçları" terimi olarak anlaşılması gerektiğini yinelemek isteriz.

suçları bununla ilgili olmakla birlikte, aslında buna bağlı olarak bilgisayar suçundan daha dar bir alanla ilgileniyoruz demektir. Benzer biçimde "dijital" ve "ileri teknoloji" suçlarının, "e-suçlar" ya da "siber suçlar" da olduğu gibi mutlaka internete bağlı olmayı gerektirmeyen daha geniş kapsamlı suçlar olduğu söylenebilir.' Bkz. A. Alisdair Gillespie, Cybercrime: Key Issues and Debates, London and New York, Routledge, 2016, s. 1 (*Aktaran* Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 147.)

389 "Bilişim suçu olarak isimlendirilen eylemler, bilgisayar üzerinde veya bilgisayar olarak nitelendirilmemekle birlikte bilgileri otomatik olarak işleme tabi tutan ya da veri iletişimi sağlayan diğer elektronik, manyetik veya mekanik araçlarla bunları veri iletişimi için birbirine bağlayan ağlar üzerinde işlenebilmektedir. Bu nedenle, 5237 sayılı TCK' da düzenlenen bilişim suçlarına "Bilişim Alanında Suçlar" denmesinin isabetli olduğu değerlendirilmektedir." Bkz. Orta, *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim),* s. 87.

390 Yazıcı' ya göre de, "… siber suç veya bilgisayar / internet suçları yerine "bilişim suçları" tabirinin kullanılması, bilişim sistemi teriminin bilgisayar ve internetten daha geniş bir alanı kapsadığı dikkate alındığında ve teknolojik gelişmelerle ortaya çıkan sistemlerin çeşitliliği karşısında yerinde bir tercih olmuştur." Bkz. Pınar Yazıcı, "Ulusal Mevzuat ve Yargıtay İçtihatları Işığında Türk Ceza Kanunu'ndaki "Bilişim Alanında Suçlar" ", Prof. Dr. Belgin Erdoğmuş'a Armağan (Derleyen: M. Murat İnceoğlu), *Der Yayınları*, İstanbul, 2011, ss. 909-928, s. 911.
"Bilişim suçu" terimini benimseyen görüşler için bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 59; Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 52; Taşkın, a.g.e., s. 12; Doğan, a.g.e., s. 16, 17; Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, s. 47; Mert Çakıcı, "Türk Ceza Kanunu M.243 ve M.244' te Düzenlenen Bilişim Suçları", *Ceza Hukuk Dergisi*, Yıl: 9, Sayı: 24, Nisan 2014, ss. 307-349, s. 310.

391 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 75; Doğan, a.g.e., s. 17.
"…Anglo Amerikan hukuk sistemlerinde ve hatta Kıta Avrupası hukuk sistemine ait bazı ülkelerde, "cybercrime" yani "siber suçlar" terimi yerleşmiş durumdadır. Ancak ben bunun yerine Türkçe bir kavram olan ve ülkemizde hem öğretide hem de mevzuatta yaygın bir biçimde kullanılan "bilişim suçları" kavramının kullanılmasının ülkemiz öğretisi ve uygulaması açısından daha uygun olduğunu düşünmekteyi." Bkz. Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 149.

1.2.2. Bilişim Suçu Kavramı ve Sınıflandırılması

Türk Hukukunda benimsenen "bilişim suçu" kavramının gerek Ceza Kanunu gerekse özel kanunlarda bir tanımı bulunmamakla[392] beraber doktrinde de kavramın tanımı üzerinde fikir birliği bulunmamaktadır[393]. Bunun yanında, bilişim suçunun tanımı, ilgili uluslararası hukuk düzenlemelerinde de yer almamakta, bunun yerine eylemlerin çeşitliliği nedeniyle ulusal ve uluslararası hukuk kaynaklarında suçların sayılması yoluna gidilmektedir.[394] Nitekim, Avrupa Konseyi Siber Suçlar Sözleşmesi' nde (Sanal Ortamda İşlenen Suçlar Sözleşmesi) de tanımlama yapmak yerine suçlar belirlenmiştir.[395] Karagülmez, bilişim suçlarının başlangıçta geleneksel suçların bilgisayar yoluyla işlenmesi olarak kabul edilirken zamanla teknolojinin getirmiş olduğu önceki suç tanımlarına benzemeyen yeni suç tiplerinin ortaya çıktığını, bilişim suç tiplerinde yaşanan çeşitlilik ve sürekli artış sonucunda bu suçlara tek bir tanımın yeterli olmayacağını belirtmektedir.[396] Esasen, "bilişim suçları" adı altında işlenen suçlar, bilişim sistemlerinin ceza mevzuatlarına etkisi bakımından belirli bir dönemde ceza mevzuatlarında yer verilen suçlar olup hali hazırda ceza mevzuatlarında yer alan bazı suçların da "bilişim suçları" adı altında incelenmesi ise, söz konusu suçların işlenme yoğunluğunun bilişim sistemlerinin kullanımı ile artmasından kaynaklanmaktadır.[397] Ancak doktrinde, hukuk alanına yeni dahil olmuş bilişim suçları gibi teknik bir olgunun multi-disipliner bir yaklaşım içerisinde ilgili alanların

---

392 Orta, *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim),* s. 85.

393 Erdoğan' a göre, bilişim suçunun tanımındaki görüş ayrılıkları, "bilgisayar" terimi üzerinde uzlaşılmış bir tanımın olmaması, uygun tanımlama için gerekli olan adli ve teknik boyutlardaki sorunlar hakkında kapsamlı bir bilginin olmayışı ve sürekli gelişen bilişim teknolojisi karşısında hangi eylemlerin bilişim suçu olduğu hususunda uluslararası ortak bir tavrın geliştirilememiş olunmasıdır. Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 47.

394 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 75.
Gerçekleştirilen hareketlerin heterojenliği sebebiyle bilişim suçlarını oluşturan eylemlerin sayılması yoluna gidildiği belirtilmektedir. Bkz. Akbulut, Bilişim Alanında Suçlar, s. 55.

395 Sözleşmeyi hazırlayanların siber suç kavramı ile ilgili taraf devletlerde ortaya çıkacak yorum farklarını ortadan kaldırmayı amaçladıkları doktrinde belirtilmiştir. Bkz. Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* s. 51, 52.

396 Karagülmez, a.g.e., s. 44.

397 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 38, 39. Aynı yönde bkz. Orta, *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim),* s. 84.
Ketizmen, bilişim suçlarına (veya bilgisayar suçları) ilişkin bir tanım yerine bu ad altında işlenen suçların, bilişim ya da bilgisayar sistemlerinin kullanılmasının belirli bir dönemde ceza hukukuna etkisi olarak nitelendirmeyi uygun görmekte ve suçta kullanılan araç ya da suçun maddi konusunun bilişim ya da bilgisayar sistemlerinin esas alınarak tanımlanmasının suçun hukuki konusu farklı olan birçok suçun da bilişim ya da bilgisayar suçu olarak toplu bir şekilde incelenmesi anlamına geleceğini belirtmektedir. Bkz. A.e., s. 38.

uzmanlarıyla gerçekleştirilecek ortak çalışma sonucunda aydınlatılması ve tanımlama kriterlerinin belirlenmesi gerektiği de belirtilmektedir.[398] Nitekim, Karagülmez de bilişim suçu türlerinin sürekli artması karşısında, üzerinde anlaşma sağlanabilen bir tasnifin bile yapılamamasının kriminolojik açıdan bu suçların ele alınmasında önemli bir zorluk oluşturduğunu belirtmektedir.[399]

ABD' de bilgisayar aracılığıyla işlenen suçlar alanındaki ilk hukuki düzenleme olan 1978- Florida Bilgisayar Suçları Kanunu' nun yapımında etkin rol oynayan Don Parker' a göre suçlar; bilgisayarın nesne olarak yer aldığı suçlar, bilgisayarın süje olarak yer aldığı suçlar, bilgisayarların suçun işlenmesinde ve planlanmasında araç olarak kullanıldığı suçlar ve bilgilerin kendisinin kullanıldığı suçlar şeklinde dörde ayrılarak sınıflandırılmaktadır.[400] 11.06.1999 tarihinde Birleşmiş Milletler ve Avrupa Birliği tarafından hazırlanan "Bilişim Suçları Raporu" na göre ise suçlar, "Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme", "Bilgisayar Sabotajı", "Bilgisayar Yoluyla Dolandırıcılık", "Bilgisayar Yoluyla Sahtecilik", "Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" ve "Yasadışı Yayınlar" başlığı altında diğer suçlar olarak altıya ayrılarak sınıflandırılmaktadır.[401] OECD' nin bilgisayar suları ile ilgili ceza yasalarının birbirleriyle uyumlaştırılması çalışmalar sonucunda

398 Erdoğan, bir konunun tanımının, o konu hakkında izlenecek yasal tutumu belirlemede ve özellikle teknik bir konu olan bilişim suçlarında kullanılan kavramların taşımakta oldukları anlamların önemli olduğu, zira kavramlara farklı anlamlar yüklenilmesinin kanunilik ilkesi uyarınca failin cezalandırılabilirliğini etkileyebileceğini belirtmektedir. Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 47.
Doğan da, daha kapsamlı ve yeni teknolojiler sayesinde ortaya çıkabilecek yeni eylemleri de kapsamaya çalışan bir tanımın yapılması gerektiğini belirtmektedir. Bkz. Doğan, a.g.e., s. 16.
Kurt' a göre de "bilişim suçu" tanımını yapmak suç kapsamına hangi eylemin girdiğini tespit bakımından önem taşımaktadır. Bkz. Kurt, a.g.e., s. 49.
Dülger' e göre de, "bilişim alanındaki hızlı gelişimi dikkate alan ve yeni teknolojiler sayesinde ortaya çıkabilecek yeni eylen türlerini de kapsamaya çalışan, bir başka deyişle sınırlı olmayan ucu açık bir tanımın yapılması için çalışılması doğru bir yaklaşımdır. Ancak bu yapılırken ceza yasalarında yer alan ve geleneksel suç tiplerinden hiçbir farkı olmayan bir suçu da sırf suçun bir işleniş modelinde bilişim sistemleri kullanılıyor diye (örneğin internet üzerinden yapılan hakaret suçu) bilişim suçu olarak değerlendirmeye neden olacak genişlikte bir tanımın yapılmasından kaçınılmalıdır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 77.
Ancak Dülger başka bir çalışmasında ise şu hususu belirtmiştir: "…Bu alandaki bir isimlendirme ya da sınıflandırma çalışmasının amacı, bu alanın olduğu gibi tanımlanmaya kalkışılmasından ziyade, siber uzayda hali hazırda gerçekleşen farklı türdeki suç aktivitelerinin etkin bir biçimde incelebilmesi için bir çerçeve sağlanmasıdır." Bkz. Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 149.
Pallı, bilişim suçlarının, geleneksel suçların bir bölümünü ilgilendirmesinden başka bu alanda yeni suç tiplerini barındırması nedeniyle kanunilik ve belirlilik ilkeleri uyarınca somut şekilde ortak tanımlarının yapılmasının bir zorunluluk olarak karsımıza çıktığını belirtmektedir. Bkz. Pallı, a.g.e., s. 41.
399 Karagülmez, a.g.e., s. 49.
400 Özen ve Baştürk, a.g.e., s. 89, 90.
401 Demircan, a.g.e., s. 25; Orta, *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim),* s. 86.

yayınladığı "Computer-Realted Crime: Analysis of Legal Policy" raporuna göre cezai müeyyide ile karşılanması gereken ihlaller, bilgisayar yoluyla dolandırıcılık, bilgisayar yoluyla sahtecilik, bilgisayar program ve verilerinde değişiklik yapılması, bilgisayar programlarının telif haklarına aykırı olarak kopyalanması, çoğaltılması ve dağıtılması ve telekomünikasyon sistemlerinin, bilgisayarların diğer fonksiyonların ve iletişimin değişikliğe uğratılmasıdır.[402] Avrupa Konseyi Siber Suçlar Sözleşmesi' nde ise bilişim suçları, bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar, bilgisayarla ilişkili suçlar, içerikle ilişkili suçlar ve fikri mülkiyet haklarının ihlali ile ilgili suçlar olmak üzere dörde ayrılarak sınıflandırılmıştır.[403] Avrupa Ekonomik Topluluğu' nun 1983 yılı Paris toplantısında yapmış olduğu (genel kabul gören) tanımında ise bilgisayar suçları, "bilgileri otomatik işleme tâbi tutan veya verilerin nakline yarayan bir sistemle gayrı kanuni, gayrı ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır."[404] Akbulut' a göre ise tanımlamada ileri sürülen yedi kriter bulunmakta olup bunlar bilgisayarın veya bilişimin amaç veya araç olmasını arayan kriter, suçları malvarlığı ihlalleriyle sınırlayan kriter, bilişim sistemleriyle herhangi bir şekilde bağlantılı olan suçları esas alan kriter, bilgisayar veya bilişim araçlarının kullanımını esas alan kriter, suçu işleyen faili esas alan kriter, veri iletişim ağlarını esas alan kriter ve tanım yapmayanların suçları gruplandırmasıdır.[405] Doktrinde yer alan bir görüşte ise terminolojideki farklılıklar ve bunların neleri kapsadığı hususunda artık bir uzlaşmaya varıldığı siber suçların "yalnızca bir bilgisayar, bilgisayar ağı ya da bir başka tür ICT kullanılarak işlenebilen"[406] "sibere bağlı/cyber-dependent" ve "bilgisayarlar, bilgisayar ağları ya da bir başka tür ICT kullanılarak işlenen ya da işlenme oranı artan geleneksel suçlar"[407] "siber sayesinde/cyber-enabled" işlenen suçlar olmak üzere iki ilke kategorisi bulunduğu belirtilmektedir.[408]

402 Yasin Beceni, Siber Suçlar, IV. Bölüm, s. 5, 6, http://www.hukukcu.com 03.04.2004 (*Aktaran* Eker, a.g.e., s. 109)
403 Orta, *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim),* s. 86, 87.
404 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 49; Karagülmez, a.g.e., s. 46; Kurt, a.g.e., s. 50.
405 Akbulut, *Bilişim Alanında Suçlar*, s. 59- 67.
406 "Bunlar sıklıkla bilişim yazılımları, kötücül yazılımlar veya DoS atakları gibi, teknolojinin suç aktivitelerinin hedefinde olduğu suçlarla ilgilidir." Bkz. Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 148.
407 "Örneğin, çocuk pornografisi, takipçi tacizci (stalker), fikri mülkiyet hırsızlığı ya da dolandırıcılık gibi." Bkz. A.e.
408 A.e.

Doktrininde yer alan bilişim suçları tanımlarına bakmak gerekirse, Kurt bilişim suçlarını, *"verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içinde işlenen, bir bilgisayar ya da ağına yönelik olarak ya da onları kullanarak icra edilen her türlü yasadışı haksız eylem"*[409] olarak ifade etmektedir. Doğan' a göre bilişim suçu, *"bilişim sistemleri ya da araçları kullanılarak bilişim sisteminin kendisine veya bilişim sistemindeki verilere yahut veri işlemle bağlantısı olan sistemlere karşı hukuka aykırı olarak gerçekleştirilen eylemlerin bütünü"*[410] olarak tanımlanabilmektedir. Apaydın' a göre, bilişim suçları, *"bilişim sistemlerine yasa dışı olarak erişimde bulunarak, bilişim sistemleri aracılığıyla bu sistemde yer alan veri ya da verileri yetkisiz bir şekilde hukuka aykırı olarak kendisinin ya da başkasının yararına kullanma, erişilmez kılma, silme, değiştirme veya bozma suretiyle işlenen suçlar"* olarak tanımlanabilmektedir.[411] Yetim, bilişim suçlarını, bilgisayar ve network hatlarının güvenliğini ve güvenilirliğini ihlal eden sınır tanımayan modern suçlar olarak tanımlamakta ve TCK' da yer alan sistemlere izinsiz erişim, veri ekleme, silme gibi çeşitleri örnek vermekte, bir kısım suçların ise dolaylı olarak bilişim sistemlerini hedef aldığını, haberleşmenin ve özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi gibi suçların "bilişim vasıtası kılınarak işlenen suçlar" olduğunu savunmaktadır.[412]

Üçüncü bir kategorinin ise "bilgisayar destekli/ computer suported" olduğu, bu suçların işlenmesinde bilgisayarın kullanılmasının rastlantısal olup bunların suça ilişkin önemli deliller sağlayabildiği belirtilmektedir. Bkz. A.e.

409 Kurt, a.g.e., s. 53.

410 Doğan, a.g.e., s. 16, 17.

411 Apaydın, "Bilişim Sistemine Girme Suçu", s. 251; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 209.

Apaydın bunun yanında 5237 sayılı TCK' nın bilişim suçlarını "Bilişim Alanında Suçlar" başlığı altında düzenlemekle yetinmediğini, bilişim sistemlerinin araç olarak kullanıldığı mevcut suçların nitelikli hallerine de yer verdiğini belirtmektedir. Bkz. A.e.

412 Yetim, bilişim suçlarını doğrudan bilişim suçları ve bilişim vasıta kılınarak işlenen suçlar olarak ayırmakta ve "doğrudan bilişim suçu sayılmayan, fakat bilişim vasıtası kılınarak işlenen "haberleşmenin gizliliğini ihlal", "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması", "özel hayatın gizliliğini ihlal", "kişisel verilerin kaydedilmesi ve izinsiz olarak ele geçirilmesi" gibi suçların da bilişim vasıta kılınarak işlenmesi durumunda ise ayrıca bir düzeleme yapılmaksızın TCK'daki düzenlemeler yeterli görülmüştür." hususlarını ifade etmektedir. Bkz. Yetim, a.g.e., s. 81. Yazıcı da, bilişim teknolojisinin geniş çerçevesi dikkate alındığında, 5237 sayılı TCK' nın 243. ve devamı maddelerinde düzenlenen suçlar dışında bilişim suçları ile ilişkilendirilebilecek başka suçların da bulunduğunu, bu bağlamda 5651 sayılı Kanun' un 8. maddesinde belirtilen internet ortamında işlenebilecek suçların da içerik suçu olarak bilişim suçları kapsamında olduğu, TCK' nın ikinci kısım dokuzuncu bölümünde düzenlenen "özel hayata ve hayatın gizli alanına karşı suçlar" ile Türk Ticaret Kanunu, Elektronik İmza Kanunu, Sermaye Piyasası Kanunu, Bankacılık Kanunu, Terörle Mücadele Kanunu ve Fikir ve Sanat Eserleri Kanunu hükümlerinin de bilişim suçu söz konusu olduğunda göz önünde tutulması gerektiğini belirtmekte, bilişim suçları alanında yapılan "doğrudan bilişim suçu" – "dolayısıyla bilişim suçu" ayrımı gözetildiğinde TCK 243 ve devamında düzenlenen suçların ilk kategoriye, klasik suçların bilişim sistemlerinden yararlanılarak işlenmesini içeren TCK m. 112, 113, 125, 132, 142/2-e, 158/1-f, 213-218, 226, 228 vb. suçların ise ikinci kategoriye giren suçlar kapsamında sayılacağını belirtmektedir. Bkz. Yazıcı, a.g.e., s. 911, 912.

Değirmenci' ye göre bilişim suçlarını klasik suçlardan ayıran özellik, bu suçların verilerle veya veri-işlemle ilgili olması olup bu suçlar her ne şekilde tasnif edilirse edilsin temelde iki şekilde işlenebilmektedir. Bunlardan biri failin, bir bilişim sisteminde bulunan verileri, programları ya da ele geçirmeyi amaçladığı diğer herhangi bir unsuru hedef alması, ikincisi ise suçun işlenmesinde failin bilişim sistemini vasıta olarak kullanmasıdır.[413] Karagülmez, bilişim suçu tanımının belli bir süre kapsayıcı olabilmesi için genel bir yapıda olmasında yarar olduğunu belirterek bilişim suçunu, "bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suç" olarak tanımlamakta[414] ve bilişim suçlarını geniş anlamda, bilgisayarın fiziki yapısına zarar verme fiilleri, bilgisayarın tek başına çalışma sistemine ilişkin fiiller, bilgisayar ağlarına yönelen bir başka deyişle internet ortamında ya da internet yoluyla işlenen fiiller olarak üç ana başlıkta ele almaktadır.[415] Özen, Baştürk' e göre ise, bilişim suçlarına ilişkin farklı sınıflandırmalar bulunmakta ise de hangi ayrım kabul edilirse edilsin bu suçlar için ortak unsur, bilgisayarın veya bilgisayar sistemlerinin suçun işlenmesinde araç olarak veya hukuki konu olarak yer almasıdır.[416]

Türk Hukuk Doktrininde bilişim sistemleri aracılığıyla işlenebilen suçlar ve bilişim sistemlerine özgü suçlar olmak üzere genellikle ikili ayrım ile yapılan sınıflandırma tercih edilmekte[417] başka sınıflandırmalara[418] da rastlanmaktadır. Taşkın' a göre, bilişim suçları temelde iki şekilde işlenebilmekte olup bunlardan birincisi bilişim sistemlerine karşı işlenen suçlar, ikincisi ise bilişim sistemleri aracılığıyla işlenen suçlardır.[419] Mahmutoğlu' na göre bilişim suçları üçe ayrılmakta olup bunlar, sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar (doğrudan ya

413 Değirmenci, "Bilişim Suçları", s. 61.

414 Karagülmez, a.g.e., s. 46.

Aydın' a göre de bilişim suçu tanımları bilişim sistemlerine karşı işlenen suçlar ve bilişim sistemleri ile işlenen suçlar olmak üzere iki ayrı düzeyde incelenebilir. Ayrıntılı bilgi için bkz. Emin Doğan Aydın, "Bilişim Sistemlerinde Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları", *Marmara İletişim Dergisi*, Sayı: 1, Aralık 1992, ss. 109-137, s. 120- 125, https://dergipark.org.tr/tr/download/article-file/2664, ET. 16 Mart 2020.

415 Karagülmez, a.g.e., s. 61.

416 Özen ve Baştürk, a.g.e., s. 91

417 Karagöz, a.g.e., s. 66.

418" Veri Suçları, Ağ Suçları, Yetkisiz Giriş Suçları ve İlgili Suçlar" Ayrıntılı bilgi için bkz. Değirmenci, "Bilişim Suçları", s. 119-125.

419 Taşkın, TCK' da yer alan bazı suçların bilgisayar aracılığıyla işlenmesinden ibaret olabileceği gibi sadece bilişim sistemlerine karşı işlenen suçlar da olabileceğini, hırsızlık suçunun bilişim sistemi aracılığıyla işlenmesi halinde bilişim sistemi aracılığıyla gerçekleştirilen bu eylemin hırsızlığın sadece bilgisayar aracılığıyla işlenmiş olan bir türü olduğu, şifre kırma eylemlerinin ise özünde yasada tanımlanmış olan başka bir suçun ağırlaştırılmış biçimi olmadığı, sadece bilişim sistemleri aracılığıyla işlenebilen suçlardan olduğu, bu nedenle "Bilişim Alanında Suçlar" başlığı ile ayrıca düzenlendiğini ve bunun doğru olduğunu belirtmektedir. Bkz. Taşkın, a.g.e., s. 11, 12.

da dar anlamda veya gerçek bilişim suçları), bilişim sisteminin kullanılması zorunlu olmamakla birlikte bazı suçların nitelikli hali olan suçlar ve kanunda bu sistemin kullanılması zorunlu olmamakla birlikte söz konusu sistemin suçta vasıta olarak kullanıldığı suçlardır.[420] Doktrinde yer alan bir başka sınıflandırmada ise bilişim suçları, veri suçları (verilerin durdurulması, değiştirilmesi, çalınması), ağ suçları (ağ engellenmesi, ağ sabotajı) ve ilgili suçlar olarak ayrılmıştır.[421] Eker' e göre, bilişim suçları, bilişim araçlarına (veya sistemlerine) karşı veya bilişim araçları (veya sistemleri) vasıtasıyla işlenen, verilerle, veri-işlem ile veri-aktarımıyla ilgili olan suç şekillerine karşılık gelmektedir.[422] Pallı' ya göre ise bilişim suçları asgari düzeyde bilişim sistemlerine yetkisiz erişim, sisteme zarar verme, bilişim sistemleri vasıtasıyla dolandırıcılık, bilişim sistemleri vasıtasıyla sahtecilik, bilgisayar programlarına ilişkin telif hakları ihlâli, verilerle ilgili suçlar, zararlı bilgisayar programlarının üretimi ve dağıtımı, bilişim sistemleri vasıtasıyla çocuk pornografisi, siber terörizm, yasak internet yayıncılığı, bilişim sistemleri vasıtasıyla tehdit, hakaret ve kumar oynama, bilişim sistemleri vasıtasıyla insan ticareti, bilişim sistemi hizmetlerinden karşılıksız yararlanma gibi suçlardır.[423]

Erdoğan' a göre bilişim suçlarının bazıları sadece bilişim alanında işlenebildiğinden bazılarının ise kısmen somut dünyada gerçekleşmesi sebebiyle bilişim suçlarının tanımı yapılırken ikili bir ayrım yapılması gerekmekte olup dar anlamda bilişim suçları, *"bilişim sisteminin kendisinin ya da bilişim sistemi içerisinde bulunan verilerin hedef alındığı ve bilişim teknolojilerinin kullanılması suretiyle ya da bilişim*

420 Mahmutoğlu' na göre TCK 243, 244 ve 245. maddelerde düzenlenen suçlar, sadece bilişim sisteminin kullanılmasıyla işlenebilen suçları, TCK 142/2-e ve TCK 158/1-f maddelerinde düzenlenen suçlar, bilişim sisteminin kullanılması zorunlu olmamakla birlikte bazı suçların nitelikli hali olan suçları, TCK 132, 124, 112, 113, 125, 226, 228, 214, 105 gibi suçlar ise kanunda bu sistemin kullanılması zorunlu olmamakla birlikte söz konusu sistemin suçta vasıta olarak kullanıldığı suçları oluşturmaktadır. Bkz. Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt: LXXI, Sayı:1, Yıl: 2013, ss. 855-888, s. 856. Aynı yönde görüş için bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 77.

421 Ayrıntılı bilgi için bkz. Demircan, a.g.e., s. 23- 30.

422 Eker, a.g.e., s. 105.

423 "Bu noktada Türk Ceza Kanunu'nda müstehcenlik suçu adı altında düzenlenen suç tipi de şayet bilişim sistemleri kullanılarak gerçekleştirilmişse bilişim suçu kapsamında değerlendirilecektir. Fakat gerek pornografi gerekse müstehcenlik suçunu oluşturan diğer eylemlerin uluslararası düzeyde suç olarak kabul edilmesi devletler açısından zorunlu olmayacak, isteğe bağlı bilişim suçları olarak değerlendirilebilecektir. Ama bu gelecekte bilişim suçlarıyla ilgili olarak uluslararası düzeyde yapılacak yeni bir sözleşmeye taraf olan devletlerin ortak kabulüne göre değişebilecektir. Örneğin, her nevi pornografinin bilişim sistemleri vasıtasıyla yayılmasının imzacı devletlerce kabul edilmesi zorunlu görülerek bu eylemlerin internet ortamında gerçekleştirilmesi suç sayılabilecektir." Bkz. Pallı, a.g.e., s. 44, 45.

araçlarına doğrudan fiziki müdahaleyle işlenen suçlardır", geniş anlamda bilişim suçları ise *"herhangi bir şekilde suçun icrasında bilişim sistem ya da araçlarının kullanıldığı ya da bilişim sistemlerinin veya içindeki verilerin hedef alındığı suçlardır"* şeklinde tanımlanabilmektedir.[424] Akbulut da bilişim suçlarını dar anlamda ve geniş anlamda bilişim suçları olarak ikiye ayırmakta, dar anlamda bilişim suçlarını verilerle veya veri işlemle konu bağlantısı olan, bilişim sistemleriyle veya bilişim sistemlerine karşı işlenen suçlar olarak tanımlamakta bunlara bilişim teknolojisinin ortaya çıkardığı suçların (bilişim sistemine girme, sisteme yetkisiz müdahale, verilere müdahale gibi) girdiğini geniş anlamda bilişim suçlarının kapsamına ise mevcut suçların bilişim araçlarıyla gerçekleştirilmesi dahil (propaganda, tehdit, hakaret, pornografik yayınlar vb.) tüm ihlal şekillerinin girdiğini belirtmektedir.[425] Dülger de bilişim suçlarını dar ve geniş anlamda olmak üzere iki şekilde incelemekte ve dar anlamda bilişim suçunu "*verilere ve/veya bilişim sistemlerine veya sistemin/verilerin düzgün ve işlevsel işleyişine, güvenliğine ya da bütünlüğüne karşı işlenen suçlar",* geniş anlamda bilişim suçunu ise *"bilişim sistemlerinin ve/veya verilerin kullanıldığı ya da bu sistem ya da verilere karşı işlenen her türlü suç"* olarak tanımlamaktadır.[426] Demircan ise Ceza Kanunumuzun bilişim suçlarını "bilişim sistemlerine karşı suçlar" ve "bilişim sistemleri aracılığıyla işlenen suçlar" sınıflandırmasını tercih ederek karma sistemi benimsediğini belirtmektedir.[427] Gül ise bilişim suçlarını doğrudan ve dolaylı bilişim suçları olarak tasnife tutmaktadır.[428] Yargıtay ise 2007 tarihli kararında: *"...Bilişim suçu verilere karşı ve /veya*

424 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* s. 53.

425 Akbulut, *Bilişim Alanında Suçlar*, s. 69, 70.

426 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 77, 78.
"Birleşmiş Milletler 10. Kongresinde de suçları, dar anlamda bilişim suçları ve geniş anlamda bilişim suçları olmak üzere iki alt kategori içinde değerlendirilmektedir. Dar anlamda bilişim suçları bilişim sisteminin güvenliğini veya veri işlemini hedef alan eylemlerdir. Geniş anlamda bilişim suçları ise bilişim sistemi ve ağı marifetiyle bu sistem veya ağda gerçekleşe herhangi hukuk dışı eylemlerdir." Bkz. Fatma Burcu Nacar, *Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları*, Atılım Üniversitesi Sosyal Bilimler Enstitüsü Avrupa Birliği Anabilim Dalı Yüksek Lisans Tezi, Ankara, 2010, s. 13, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.
Dülger' e göre bilişim alanındaki hızlı gelişim sebebiyle ortaya çıkabilecek yeni eylem türlerini de kapsayabilmesi açısından sınırlı olmayan ucu açık bir tanım doğru bir yaklaşım olmakla birlikte geleneksel suç tiplerinden hiçbir farkı olmayan bir suçun da sırf suçun işlenişinde bilişim sistemleri kullanılıyor diye bilişim suçu olarak değerlendirmeye yönelik bir suç tanımından kaçınmak gereklidir. Bkz. A.e., s. 77.

427 "…açıktır ki kanun koyucu bilişim suçlarını ayrı bir kanunla düzenlemek yerine yine karma bir yolu / yöntemi tercih ederek hem Ceza Kanununa bilişim suçlarını düzenlemek amacıyla yeni hükümler eklemiş hem de klasik / geleneksel suç tiplerini düzenleyen normların ihlalini düzenlerken bu suçların işleniş biçimlerini çeşitlendirerek bilişim suçlarına vücut veren yeni fiiller / modaliteler eklemiştir." Bkz. Demircan, a.g.e., s. 65.

428 "Yine TCK 142/2-e maddesinde düzenlenen "bilişim sistemlerinin kullanılması suretiyle hırsızlık" ve TCK 158/1-f maddesinde düzenlenen "bilişim sistemlerinin araç olarak kullanılması

veri işlemle bağlantısı olan sistemlere karşı bilişim sistemleri aracılığıyla işlenen suçlar"[429] şeklinde tanımlamıştır.

Yasa koyucular, yapısı gereği çok dinamik ve değişken olan bilişim alanında gerçekleştirilen haksız eylemlerin tanımlanmasından mümkün olduğunca uzak dursalar da kanunların öncelikle suçun maddi unsurlarının belirlenmesi yolu ile yapılması sonucunda suçların temel hatlarını belirlemekten uzak duramamışlardır.[430]

Kanaatimizce, Dülger' in de belirtmiş olduğu gibi bir suçun işlenmesinde sadece bilişim sistemlerinin araç olarak kullanılması o suçu "bilişim suçu" olarak kabulü anlamına gelmemelidir. Zira, teknolojinin gelişmesiyle birlikte önceden öngörülmesi pek mümkün olmayan, fiziki varlığı bulunmayan ve aslında dijital olarak nitelendirilebilecek hareketlerle oluşan ihlallerin ortaya çıkışı, başka bir deyişle bu eylemlerin klasik suç tiplerinden farklı oluşu söz konusu eylemlerin ayrıca ve farklı suç tipi olarak düzenlenmesi ve kanun koyucuların bu alana ilişkin yeni düzenlemeler yapmasını sonucunu doğurmuştur.[431] Başka bir deyişle, bilişim suçlarının ayrı suç tipleri olarak düzenlenmesi ve incelenmesi, diğer suç tiplerinden bazı noktalarda ayrılması, farklılaşması sonucunda olmuş olup bir eylem aynı zamanda birden fazla suç tipini ihlal edip birden fazla suç tipine yakınlık gösterebilecekse de "bilişim alanında suçlar" şeklinde ayrı bir alan oluşmuş ve ayrı suç tipleri ortaya çıkmış ise söz konusu suçların diğerlerinden farklılaştığı noktalara eğilerek tanımlama ve çalışma gerçekleştirilmelidir. Bu yüzden bir suçun işlenmesi için bilişim suçlarına özgü araç, cihaz ve aygıtların kullanılması yalnızca bu sebeple o suçun bilişim suçu adı altında incelenmesi sonucunu doğurmamalıdır.[432] Günümüzde genel ve özel kısım ayrımına

---

suretiyle dolandırıcılık" suçları da cezanın ağırlaştırılmasını gerektiren nitelikli hal olarak; yani dolaylı bilişim suçu sayılabilecek şekilde düzenlenmiştir." Ayrıntılı bilgi için bkz. Gül, a.g.e., s. 25.

429 Yargıtay Ceza Genel Kurulu 10.06.2007 t., E: 2007/6-136, K: 2007/150.

430 Kurt, a.g.e., s. 60.

431 "…bilişim suçları, geleneksel ceza hukuku kavramları, müesseseleri ile kavranması güç olan yeni bir kriminolojik olgudur. Bu açıdan bilişim alanındaki hukuki ihlallerin cezalandırılabilmesi amacıyla ülkeler mevzuatlarında çeşitli düzenlemeler gerçekleştirme ihtiyacı duymuşlardır." Bkz. Eker, a.g.e., s. 107.

432 Koca, Üzülmez' e göre de, tehdit, hakaret, hırsızlık, dolandırıcılık, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi vb. çok sayıda suçun bilişim sistemleriyle işlenmesi mümkünse de bu ve benzeri suçların bilişim sistemleri aracılığıyla işlenmesi, bu suçları bilişim alanında işlenen suçlar haline getirmemekte, bu fiiller bilişim sistemleri aracılığıyla işlendiğinde de failin ceza sorumluluğu korunan hukuki değer esas alınarak kanunların ilgili bölümlerinde yapılan suç tanımlarına göre belirlenecektir. Bkz. Koca ve Üzülmez, a.g.e., s. 802.

Gül' e göre de: "Ayrıca 'bilişim alanında suçlar' başlığı altında bilişim alanında işlenebilecek suçların hepsi düzenlenmiş değildir. Esasen bu suçların hepsinin aynı bölümde düzenlenmesi de mümkün değildir. Zira bilişim sistemleri artık hayatın her alanında kullanılmaktadır…Bu nedenle örneğin tehdit, hakaret, şantaj, hırsızlık, dolandırıcılık, zimmet, sahtecilik, haberleşmenin gizliliğini ihlal, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi, suç işlemeye tahrik, halkı kin ve düşmanlığa tahrik, müstehcenlik, kumar oynanması için yer ve imkan sağlama, devlet sırlarının

yer veren ceza kanunlarının özel kısmında suç tipleri belli bir gruplandırmaya tabi tutulmuş olup Türk Ceza Kanunu sistematiğinde de ceza hukuku özel hükümler düzenlenirken suçla korunan öncelikli hukuki değere bakılarak suçların gruplandırılması yöntemi seçilmiş (suçlar üst kavramlardan (kısımlar) alt kavramlara (bölümler) ayrılarak belirlenmiş)[433] ve bilişim suçları için "Topluma Karşı Suçlar" başlıklı üçüncü kısmın onuncu bölümünde "Bilişim Alanında Suçlar" düzenlemesiyle bilişim suçu olarak kabul edilen suç tipleri ayrı bir bölüm altında düzenlemiştir.[434] Bilişim suçlarının sınırlarının açıkça belirlenmesi ve diğer suçlardan ayrımının açıkça ortaya konulmasının pek mümkün olmaması sebebiyle[435] bilişim suçları konusunda

ifşası, fikri hakların ihlali gibi çok sayıda suçun bilişim sistemleri aracılığıyla işlenmesi mümkündür. Ancak bu ve benzeri suçların bilişim sistemleri aracılığıyla işlenmesi bu suçları bilişim alanında işlenen suçlar haline getirmeyecektir. Bu fiiller bilişim sistemleri aracılığıyla işlendiğinde de failin ceza sorumluluğu, korunan hukuki değer esas alınarak kanunların ilgili bölümlerinde yapılan suç tanımlarına göre belirlenecektir." Bkz. Gül, a.g.e., s. 25.

433 Mehmet Emin Artuk, Ahmet Gökcen ve A. Caner Yenidünya, *5237 Sayılı Kanuna Göre Hazırlanmış Ceza Hukuku Özel Hükümler*, 8. Bs., Turhan Kitabevi Yayınları, Ankara, 2007, s. 4, 5.

434 Koca, Üzülmez' e göre bölüm başlığı kapsayıcı olması açısından "Bilişim Alanında Suçlar" şeklinde düzenlenmiş olup bölüm başlığı bölümde düzenlenen suçlarla korunan hukuki değeri çağrıştıracak mahiyette bulunmamakta, bölümde yer alan suçlarla ilgili bölümün başlığında korunan hukuki değere değil, suçun işleneceği alana vurgu yapılmış, bilişim alanında işlenen çeşitli suçlara, korunan hukuki değerler farklı olsa da bu bölümde yer verilmiştir. Bkz. Koca ve Üzülmez, a.g.e., s. 801, 802.

Değirmenci' ye göre: "2004 TCK'nın "Bilişim Alanında Suçlar" bölümü incelenecek olursa, 245/2. fıkrasındaki ayrık durum hariç olmak üzere düzenlenen tüm suçların ortak noktası ağırlıklı olarak bilişim sistemlerine karşı işlenen eylemlerden oluşmasıdır. Bu anlamda kanun koyucu bilişim sistemlerine karşı işlenen eylemleri "Onuncu Bölüm"de, bilişim sistemleri aracılığıyla işlenen suçları ise ihlal edilen hukuki menfaate uygun olarak ilgili maddede düzenlemiştir." Bkz. Olgun Değirmenci, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", *Türkiye Barolar Birliği Dergisi*, Sayı: 58, Yıl: 18, Mayıs-Haziran 2005, ss. 195-208, s. 201.

435 "… bilişim suçlarının sınırlarının açıkça belirlenmesi, diğer benzer konulardan ayrımının açıkça ortaya konulması mümkün değildir. Buna ek olarak, suç oluşturan bir hareket genellikle aynı anda birkaç farklı türdeki suç tipiyle uyuşmakta ya da aynı anda başka suçlarla birlikte bir suç serisinin parçası olarak işlenebilmektedir." Bkz. Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 149.

"TCK' da bilişim suçları, esas olarak "bilişim alanında suçlar" ve "özel hayata ve hayatın gizli alanına karşı suçlar" bölümünde düzenlenmiştir. Bunlar bilişim sistemiyle işlenebilen, özellikle günümüzde söz konusu sistemler kullanılmadan işlenebilme olanakları çok kısıtlı olan hatta mümkün olmayan suçlardır. Bunların yanı sıra 5237 sayılı TCK'nın çeşitli bölümlerinde bilişim sistemleri aracılığıyla suçun işlenmesine nitelikli hal olarak yer verilmiştir…Buna göre TCK'da bilişim suçu olarak nitelendirilebilecek suç tiplerinin yanı sıra bilişim sistemi aracılığıyla işlenebilen; ancak yalnızca bilişim suçu olarak tanımlanamayacak suç tipleri de yer alır. Ancak gelişen teknoloji ve yeni suç işleme modellerinin ortaya çıkması nedeniyle bu suç tipleri arasındaki ayrım net ve kesin olarak yapılamamaktadır.

…Özel hayata ve hayatın gizli alanına karşı suçlar bölümünde ise bilişim suçu olarak nitelendirilebilecek; kişisel verilerin kaydedilmesi suçu (m. 135); kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu (m. 136); verilerin yok edilmemesi suçu (m. 138) yer almaktadır.

TCK'nın çeşitli bölümlerinde bilişim sistemleriyle de işlenmesi olanaklı olan suç tipleri olarak ise; haberleşmenin gizliliğini ihlal suçu (m.132); haberleşmenin engellenmesi suçu (m. 124); hakaret suçu (m. 125); bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (m. 142/2 –e); bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu (m. 158/1-f), müstehcenlik suçu (m.226)

bir tanım yapmak yerine iki kategorili görüşün benimsenmesi gerektiği kanaatindeyiz. Bu anlamda, bir "bilişim suçu" tanımı yapılacak ise, bizce de dar ve geniş anlamda veyahut "bilişim alanında suçlar" ve "bilişim suçları" olmak üzere ikili bir ayrıma gitmek gerekmekte olup TCK' nın esas aldığı sistemin[436] mantığa da uygun olarak dar anlamda bilişim suçlarını, koruduğu öncelikli hukuki değeri verilerin ve/veya bilişim sistemlerinin işleyişi ve güvenliğine ilişkin eylemlerin oluşturduğu suçlar, geniş anlamda bilişim suçlarının ise klasik suç tiplerinin işlenişinde bilişim araç, cihaz ve aygıtlarının araç olarak olarak kullanıldığı ancak ihlal edilen öncelikli hukuki değerin ilgili başka suçlara ait olduğu suçlar olarak tanımlamak[437] doğru bir yaklaşım olacaktır. Bu doğrultuda, çalışma konumuzu oluşturan 5237 sayılı TCK' da yer alan "Bilişim Alanında Suçlar" başlığı altında düzenlenen suç tiplerini de dar anlamda bilişim suçları olarak kabul ederek çalışmamızda bu suç tiplerinin kendisine özgü yapıları doğrultusunda korudukları öncelikli hukuksal değer de dikkate alınarak incelemeler gerçekleştirilecek, konu başlıkları altında geniş anlamda bilişim suçu olarak kabul edilen diğer suç tiplerine de ilgili bölümlerinde değinilecek ve mevcut düzenlemeye öneriler getirilecektir.

1.2.3. Bilişim Suçlarının Tarihi ve Gelişimi

Bilişim suçları 1960' lı yılların sonuna dek bilinmeyen bir olgu[438] iken bilgisayarın yayılım süreci bütün tahminleri alt üst ederek geçirdiği gelişimle birlikte bilişimle ilgili suçları da ortaya çıkardı.[439] Bu yıllarda bilgisayar manipülasyonu, bilgisayar sabotajı, bilgisayar casusluğu, bilişim sistemlerinin hukuka aykırı kullanımları ile ilgili yaşanmaya başlayan çeşitli olaylar ile "bilgisayar suçları", "bilgisayarla ilgili suçlar" başlığı ile basında ve bilimsel yayınlarda bir takım yazılar çıkmaya başlamış bununla birlikte hazırlanan birçok raporda yeni yeni ortaya çıkmaya başlayan bu eylemlerin ve bu eylemlerin oluşturduğu suç tipinin faillerinin bu suçu işleme nedenlerinin neler olduğu tartışılmaya başlanmıştır.[440]

---

ve kumar oynanması için yer ve imkan sağlama (m.228/3) yer almaktadır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 234, 235.

436 "TCK, bilişim alanındaki suçları, suçun hukuki konusunu esas alan tasniften hareketle ayrı bir bölüm halinde düzenleme sistemini benimsemiş, ancak bazı fiiller açısından ise, bilişim sisteminin araç olarak kullanılmasını suçun nitelikli hali, başka bir deyişle ağırlaştırıcı nedeni saymıştır." Bkz. Özen ve Baştürk, a.g.e., s. 115.

437 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 77, 78.

438 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 53.

439 Aydın, "Bilişim Sistemlerinde Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları", s. 113.

440 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 96, 97.

Teknik anlamda bilişim suçu olarak kabul edilebilen ilk bilişim suçu, 18 Ekim 1966 tarihinde Minneapolis Tribune gazetesinde yayınlanan "bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı haber ile kamuoyuna yansımış[441] bu vaka Donn B. Parker tarafından incelenmeye başlamış ve 1970 yılında Standford Araştırma Enstitüsü' nde "Bilgisayarın Kötüye Kullanılması" isimli bir proje başlatmıştır.[442] Bilgisayar ve bilgisayara bağlı ortaya çıkan söz konusu sorunlarla ilgili ilk hukuki düzenlemeler ABD' de yapılarak Amerikan hukukunda "Computer Law" adı verilen yeni bir hukuk dalı ortaya çıkmıştır.[443] [444]

1970' li yıllarda ise daha çok bilgisayarların çeşitli şekillerde sabote edilmesi ya da casusluk faaliyetlerinde kullanılması gibi suç teşkil eden eylemlerle karşılaşılmış, zaman içerisinde bu alanda işlenen suçlar artarak daha karmaşık bir hale gelmiştir.[445] 1971 yılında Newyork-Pennsylvania merkez demiryolu hattında 200' den fazla yük vagonunun demiryolu merkez şirketinin bilgisayarlarına yapılan yetkisiz müdahaleler sonucunda rotasından sapması ve her defasında ortalama 60.000 dolarlık zarara sebebiyet vermesi[446], 1972 yılında bir mühendislik fakültesi öğrencisinin bir telefon ve bir bilgisayarın gizli giriş kodunu kullanarak yetkisiz erişim sonucunda devletin en geniş yapıdaki telefon şirketlerinden 1 milyon dolarlık elektronik ekipmanı gizlice çalması[447] bu suçlara örnek verilebilmektedir.

441 Pallı, a.g.e., s. 45; Kurt, a.g.e., s. 53; Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 53; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 97; Ayrıntılı bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 51.

442 Aydın, "Bilişim Sistemlerinde Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları", s. 113.

443 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 97.

444 Belirtmek gerekir ki, hacker'lığın tarihi gelişimi, bilişim suçlarına göre biraz farklılık gösterdiği, "Hack" kavramının ilk kez Amerika Birleşik Devletleri'nin Massachusetts Institute of Technology (MIT) Üniversitesinde ortaya çıktığı söylenmektedir. Şöyle ki, elektromekanik sistemler ile yönetilen bir model demiryolu ağı ile ilgilenen üniversitenin bir öğrenci kulübü olan Tech Model Railroad Club' de (TMRC), bazı öğrenciler işin görsel kısmıyla ilgilenip modelleri gerçeğe daha yakın yapmak için uğraşırken diğer bir grup da elektronik işlerle ilgilenmekte olup bu sistemde yapılan her yeni ilerleme ve iyileştirmeye "hack", bunları yapanlar da "hacker" adı verilmişti. Bkz. Karagöz, a.g.e., s. 63.
"Hacking, bir sistemin gizli, ulaşılamayan bilgilerini ele geçirmek demektir. Hacking işlemi aynı zamanda haklamak olarak da tabir edilmektedir. Sistemin engellerini aşarak, sisteme sızmak ve sistem sorumlularını devre dışı bırakmaktır." Bkz. Mahruze Kara, *Siber Saldırılar- Siber Savaşlar ve Etkileri*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, 2013, s. 10, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

445 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 53.

446 Karagülmez, a.g.e., s. 50.

447 Ayrıntılı bilgi için bkz. A.e.

80'li yıllarda ise virüsler sıklıkla konuşulmaya başlanmış ve 22 Ekim 1987'de de Delaware Üniversitesinde ilk virüs saldırısı gerçekleşmiş, virüs birkaç yüz dosyaya bazılarını kullanılamaz hale getirecek şekilde bulaşmıştır.[448]

1980' li yıllardan sonra ise bilgisayar ve özellikle 90' lı yıllarda internet kullanımının yaygınlaşması ile birlikte bu yollarla işlenen suçların ekonomik boyutlarının yanında en az ekonomi kadar başka değerler aleyhine de işlenebileceğinin anlaşılması ile birlikte bilişim suçu kavramı ortaya çıkarak bu suçların ayrı bir disiplin altında incelenmeye başlanmıştır.[449]

Ülkemizde ise çocukların pornografik görüntü ve resimlerini çekerek internet ağı aracılığı ile satmak iddiası ile yakalanan bir rehber öğretmenin bu konuda yakalanan ilk suçlu olduğu belirtilse de Kurt' a göre bu tespit Ceza Kanunumuzdaki bilişim suçlarının kapsamının bilinmemesi sebebiyle isabetsizdir.[450] Ülkemiz hukukunda bu alandaki ilk düzenleme, 1991 yılında 3756 sayılı Kanun ile 765 sayılı TCK'ya yeni maddeler eklenmesi ve bazı bilişim suçlarını düzenleyen "Bilişim Alanında Suçlar" başlıklı 11. babın konulması olup daha sonra 1995 yılında 4110 sayılı Kanun ile Fikir ve Sanat Eserleri Kanunu' nda (FSEK) "bilgisayar programları" da, "eser" olarak kabul edilmiş ve bilgisayar programlarına karşı gerçekleştirilen bazı eylemelerin yaptırıma bağlanmıştır.[451] Bu gelişmelerden sonra ise 2004 yılında 5070 sayılı Elektronik İmza Kanunu ile yeni suç tipleri oluşturulmuş ve son olarak 5237 sayılı Türk Ceza Kanunu' nda bilişim suçlarına ayrıntılı bir şekilde yer verilmiştir.

Günümüzde bilişim suçları çoğunlukla internet aracılığıyla ve diğer ağlar aracılığıyla işlenmekte olup internetin yaygın bireysel kullanımı ile hukuka aykırı içeriklerin dağıtılmaya başlandığı, organize suç örgütleri ile terör örgütlerinin propoganda yapmasına olanak sağlayan bir araç haline gelmiş[452] olup bu suçlarla ilgili en sorunlu alanların ise bilişim korsanlığı, bilişim sistemleri kullanılarak hukuka aykırı ekonomik yarar elde etmeye yönelik suçlar, kişisel verilere yönelik suçlar ve siber terörizm olduğu görülmektedir.[453] Bunun yanında yukarıdaki başlıklarda da belirtmiş

448 "Sistemlere zarar veren ilk virüsün ARPANet tarafından 1971 yılında Creeper adıyla oluşturulduğu söylenmektedir." Bkz. Karagöz, a.g.e., s. 64.
449 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 53, 54.
450 Kurt, a.g.e., s. 53, 54.
451 Esra Yaycı, *Bilişim Suçları*, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Ceza ve Ceza Usulü Hukuku Bilim Dalı, Master Tezi, Ankara, 2007, s. 27, 28, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.
452 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 98, 99.
453 A.e., s. 100.

olduğumuz üzere yeni teknolojilerin hızla ilerlemesinin, ortaya çıkarılan yeni ürün ve sistemlerin hukuk alanında önceden öngörülmesi ve yaptırıma bağlanması zor hukuka aykırı eylemleri beraberinde getireceği ve bu eylemlerin oluşturacağı yeni sorunların da ceza hukukuna yansıması yadsınamaz bir gerçeği oluşturmaktadır. Ceza mevzuatımızda 1991 yılından beri yapılan değişiklikler bugün için yeterli gibi gözükse de üzerinde çalıştığımız alanın dinamik yapısı göz önünde bulundurularak teknolojik gelişmeler ve yaratacağı müstakbel sorunlarla ilgili öngörü ve olasılıkların üzerine eğilerek, disiplinler arası çalışma ve bütüncül bir yaklaşımla günün gelişen şartlarının yakından takibinin gerektiği ve ilgili çalışmalara yoğunluk verilmesi gerektiği kanaatindeyiz.

1.2.4. Bilişim Suçlarının Yapısı ve Özellikleri

Bilişim sistemlerinin bünyelerinde suç yaratıcı unsurları barındırması, başka bir deyişle bu sistemlerin yapısı gereği haiz oldukları bazı özellikler,[454] bilişim suçu faillerinin bilişim ve telekomünikasyon ağlarına kolayca erişebilmeleri[455] bilişim suçlarının işlenmesi için uygun ortamı yaratma ve bu suçların işleniş oranını artırmaktadır.[456] Bilişim sistemlerinin haiz olduğu suç yaratıcı özellikler bazı yazarlara göre bilgi yoğunlaştırma, kontrol mekanizmasındaki eksikler, anonimlik olarak belirlenmiş, bazı başka yazarlara göre ise bilgisayarın verilerin komutları hiçbir sorgulamaya tabi tutmadan uygulaması, komutların insan yerine bilgisayardan geldiğinde bilgisayarın hata yapmayacağına olan inanç, para transferini çok uzak uzak mesafelerde ve çok kısa sürede yapabilmesi, suçların anonim şekilde işlenmesine olanak tanıması şeklinde belirtilmiştir.[457]

Günümüzde bankalarda gerçekleştirmiş olduğumuz bireysel işlemlerden kamusal işlerimizin e devlet uygulamasında gerçekleştirilmesine kadar birçok işlemin bilişim sistemleri kullanılarak gerçekleştirilmesi, teknoloji çağının başrolü olan bilişim suçlarının mağduru olabilme yüksek ihtimalini de beraberinde getirmektedir. Bilişim suçlarının yapısının belirlenmesi ise bu suçlar ile mücadele önemli bir hususu oluşturduğu düşünülmektedir.

454 Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", s. 2750.
455 Karagülmez, a.g.e., s. 70.
456 Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", s. 2750.
457 A.e., s. 2750-2751.

Suçun konusuna fiziken odaklanarak işlenen klasik suçlardaki fiziki yapı yerine soyut ve sanal bir alanın konu alınan veya bu alan üzerinde gerçekleştirilen bilişim suçlarının[458] kendine özgü özellikleri içerisinde öncelikle bu suçların işlenmesinin kolay ancak tespitinin oldukça zor olduğudur.[459] Bunun yanında klasik suçların etki alanı daha sınırlı ve hatta bölgesel nitelikte iken bilişim suçlarının sonuçlarını tahmin olmamakla birlikte ulusal ve uluslararası boyutları da bulunmaktadır.[460] Nitekim, bilişim suçlarının bünyesindeki ülkeler üstü işlenebilme ve sonuç doğurabilme özelliği bir devletin tek başına bu suçlarla mücadelede başarılı olabilme imkanını ortadan kaldırmaktadır.[461] Bu suçlar mekandan bağımsız ve anlık gerçekleşmekte ve işlendikten sonra ardında iz bırakmaması nedeniyle suçun maddi hareketinin tespitinde zorluk oluşturmaktadır.[462] Bu sebepledir ki söz konusu suçlar için uzmanlığı gerektiren, dinamik tedbir ve soruşturma usullerini de beraberinde gerektirmektedir.[463] Ayrıca bu suçlarda zarar görenin birden fazla kişi olması da muhtemeldir ki siber uzayda bir kimsenin kendi bilgisayarına gereken güvenlik yazılımlarını temin etmediği için bir bilgisayar korsanının saldırısına uğraması durumunda kendisinin mağduriyetinin yanında bu bilgisayar korsanının yeterli güvenlik araçları olmayan bilgisayarı zombi bilgisayar olarak kullanmak suretiyle ülkenin alt yapısına zarar vermek gibi çok daha ciddi zararlara sebep olabileceği ileri sürülmektedir.[464] Son olarak, bilişim suçlarının kolluk kuvvetlerine bildirilme oranının oldukça az ve çoğunun kamuoyuna duyurulmadığı, "köstebek" olarak adlandırılan kurum içi çalışanlar vasıtasıyla işlenmeleri, dolayısıyla takip edilememesinin de suçla mücadelede karşılaşılan bir diğer zorluk olduğu da belirtilmektedir.[465]

458 Karagülmez, a.g.e., s. 67.
459 Kurt, a.g.e., s. 56.
460 Karagülmez, a.g.e., s. 67, 68.
461 "Bilişim suçlarını böylesi bir kimlikle gerçekleştiren kişilerin, internet bağlantısı olan her ülkede yakalanıp, hakkında soruşturma başlatılabilmesi yolu açılabilir." Bkz. A.e., s. 69, 70.
462 Kurt, a.g.e., s. 57-59.
463 A.e., s. 59.
464 Pallı, a.g.e., s. 51.
465 "Şirket yöneticileri, kolluğun şirketin iç işlerine karışarak kurumun işleyişi, sırları, planları konularında detaylı bilgi sahibi olmalarını istememeleri ve bu tür bir araştırmanın şirketin piyasalarda saygınlık kaybetmesine neden olacağına inanmaları nedeniyle mağduriyetlerini gizli tutmaktadırlar. Bu durumun ise bilişim suçu faillerinin işledikleri suçun cezasız kalması sonucuna yol açtığı, böylece bu şirketlerin, daha çok fail için çekici birer hedef haline geldiği görülmektedir. Bazı şirketler, bilişim suçları sonucunda meydana gelen yıllık %5'e kadar olan zararları araştırma yapmaksızın olağan kabul etmektedirler. Tüzel kişiliklerin bilişim suçları ile mücadele etmek yerine bu suçlar dolayısıyla oluşan mağduriyetlerini sineye çekmelerinin bir tür kartopu etkisi yarattığını ve mağduriyetlerini arttırdığını söylemek mümkündür." Bkz. Damla Eryaman, *Türk Ceza Kanunu'nda Bilişim Suçları*, Çağ Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, Mersin, 2018, s. 34, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

1.2.5. Siber Güvenlik ve Siber Terörizm

Tarih öncesi dönemi de kapsayan süreç içerisinde büyük önem taşıyan, bilim ve teknolojinin geliştirilmesinde öncü rol oynayan savunma ve güvenlik kavramları[466] yanında internetin sivil kullanıma açılarak yaygınlaşması, iletişim imkanlarının gelişmesi, teknolojik yeniliklerin beraberinde getirdiği internet üzerinden yayılan zararlı yazılımların artışı "siber uzay" ve "siber güvenlik" gibi yeni kavramların tartışılmasına[467], başka bir anlatımla insanlığın sosyolojik dönüşüm evreleri boyunca ulaştığı kara, deniz, hava, uzay boyutlarına ek olarak "siber uzay" boyutunu günlük hayatımıza kazandırmış, "siber uzay" boyutunda temel ihtiyaçlar karşılanmaya başladıkça da güvenlik konusu gündeme gelerek "siber güvenlik" kavramı önem kazanmaya başlamıştır.[468] Diğer bir deyişle, oluşturulma maksadı iletişim olan interneti kullananların sayısının sınırlı olması ve bilgisayarların her eve girebilecek kadar yaygın olmayışı gibi sebeplerle bu ortamda güvenlik kaygıları olmamış ancak ilk zamanlarda internetin üzerinde var olduğu fiziksel altyapıya karşı gelebilecek tehditlerden ibaret olan endişeler sonraları zararlı kodlar ve virüslerin üretilmesi ve yaygınlaşmasıyla beraber tehlikenin seviyesi de artmaya başlamış, zamanla ekonomik sistemlerin, ticaretin ve bilgi sistemlerinin internete entegre ve bağımlı hale gelmeleri ile ve de teknolojide yaşanan gelişmelerin sistemlere yetkisiz erişim, bilgi hırsızlığı ve hatta fiziksel zararlar vermeye olanak sağlamasıyla siber uzayda güvenlik ciddi bir sorun haline gelmiştir.[469]

Siber ortamda, karşı tarafın bilgilerine ve bilgi sistemlerine yönelik zarar verme veya olumsuz etkileme istek ve ihtiyaçları "Siber saldırı – Siber taarruz", bilgi ve bilişim sistemlerinin kötü niyetli hareketlere ve saldırılara karşı korunması ihtiyacı ise "Siber güvenlik - Siber savunma" kavramlarını ortaya çıkarmış, devletler siber savunma ve siber taarruz konularında strateji ve politikalar geliştirmeye ve bunları etkinlikle uygulamaya başlamış, bunlarla birlikte de 'siber savaş' kavramı ortaya

466 Ahmet Naci Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, Nobel Akademik Yayıncılık, Ankara, 2015, s. iii (Ön Söz).
467 Ali Burak Darıcılı, *Siber Uzay ve Siber Güvenlik Nedir? (ABD' nin Siber Güvenlik Stratejisi Rusya Federasyonu' nun Siber Güvenlik Stratejisi),* Dora Basım-Yayın, Bursa, 2017, s. 1.
468 Ünal, a.g.e., s. iii (Ön Söz).
469 Mehmet Nesip Öğün ve Adem Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri*, Yıl: 9, Sayı:18, s. 150, 151, http://afyonluoglu.org/PublicWebFiles/Reports-TR/Akademi/Makale-2013-Siber%20G%C3%BCvenli%C4%9Fin%20Milli%20G%C3%BCvenlik%20A%C3%A7%C4%B1s%C4%B1ndan%20%C3%96nemi%20ve%20Al%C4%B1nabilecek%20Tedbirler.pdf, ET. 01 Şubat 2020.

çıkmıştır.[470] "Siber" ön eki eklenmek suretiyle kullanılan kavramlar genel olarak kişisel bilgisayarlar ve özellikle de internet ile bağlantılı olgular olup bu kavramlara gerçek niteliğini kazandıran şey çeşitli teknolojiler ve ağlar üzerinden "siber uzay" ile kurmuş oldukları ilişkidir. "Siber güvenlik" söz konusu olduğu zaman ise, benimsenen genel yaklaşıma göre özellikle çok daha büyük elektronik sistemlerin ve enformasyon sistemlerinin de siber güvenliğin kapsamına girdikleri yönündedir.[471] Biz de çalışmamızın bu bölümünde siber uzay, siber güvenlik, siber saldırı, siber terörizm, siber savaş kavramlarını ortak dil kullanımı açısından açıklayarak değerlendirmelerde bulunacağız.

1.2.5.1. Siber Uzay

Çağımızın en önemli varlıklarından biri olarak kabul edilecek olan bilginin, bilişim sistemlerinin sağladığı imkânlarla, işlenmesinde, iletiminde, korunmasında ve kullanılmasında sağlanan etkinliğin her geçen gün daha da artması ile yaşanan gelişmelerin paralelinde devletlerin özellikle ekonomik, politik ve askeri güçlerindeki kısa sürede meydana gelen olumlu yükselişler, kara, deniz, hava ve uzay ortamlarından sonra ortaya çıkan ve 5'inci Harekât Alanı olarak da adlandırılan Siber Ortamın önemini daha da artırmıştır.[472]

İngilizcede çoğunlukla "siber uzay" (cyberspace) olarak kullanılan, Türkçede ise "siber ortam" kavramının da kullanıldığı[473] "siber uzay", *'bilginin elektromanyetik formda oluşturulması ile başlayıp dünyanın dört bir yanını kuşatan çeşitli sistemler vasıtasıyla bilgiye erişimin sağlandığı sanal ortamın bütünü'*[474] olarak tanımlanmıştır. Başka bir tanımda ise internetten fazlası olduğu, yalnızca donanım, yazılım ve bilgiden değil aynı zamanda ağ içerisindeki sosyal etkileşimlerden de oluştuğu ifade edilen ve sanal bir bilgisayar dünyası olarak da düşünülebilen "siber uzay" kavramı, günlük hayatı

470 Mustafa Şenol, "Türkiye' de Siber Saldırılara Karşı Caydırıcılık", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, S:1-9, Cilt:3, No:2, 2017, s. 1, https://docplayer.biz.tr/146120164-Turkiye-de-siber-saldirilara-karsi-caydiricilik.html, ET. 9 Şubat 2020.

471 Soner Çelik, "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *Akademic Review of Humanities and Social Sciences,* Vol:1, Issue:2, Year:2018, pp. 110-119, s. 113.

472 Şenol, a.g.e., s. 1.

473 Bilgisayar ve ondan kaynaklanan iletişim alanını ifade etmekte kullanılan bu ortamı ifade etmek için siber uzay, sanal âlem, elektronik ortam, bilişim alanı veya internet ortamı kavramlarının kullanıldığı ve hatta güncel hayatta, akademik çevrelerde veya yasal düzenlemelerde farklı terimlerin tercih edildiği görülmektedir. Bkz. Pallı, a.g.e., s. 37.
"Yazıcıoğlu ise buna bilişim alanı demekte ve bilişim alanını bilgisayarları da kapsayan ve özellikle bilgisayar ve bu tür aygıtların yer aldığı bir alan olarak tanımlamaktadır." Bkz. a.e.

474 Ahmet Özpehlivan, "Siber Terörizmle Mücadelede Kolluğun Rolü", Kara Harp Okulu Savunma Bilimleri Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2006, s. 10 (*Aktaran* Çakmak, Demir, a.g.e., s. 27)

devam ettirecek hizmetleri sunabilen global bilgisayar ağını oluşturabilmek amacı ile kurulan elektronik bir ortam[475] olarak ifade edilmiştir. Avrupa Birliği (AB) Komisyonu' nun 2013 yılındaki tanımında, *'Dünya çapında kişisel bilgisayarların elektronik verilerinin dolaştığı sanal ortamdır.'*[476] şeklinde ve NATO' nun 2015 yılı tanımında ise, *'Bilgisayar ağları kullanılarak veri saklama, değiştirme ve takas etme amacıyla bilgisayarların ve elektromanyetik spektrumun kullanıldığı, fiziksel ve fiziksel olmayan bileşenlerden oluşan ortamdır.'*[477] şeklinde tanımlanmıştır. Bu bağlamda siber ortamın verilerin depolandığı cihazlar (fiziksel araçlar) ve iletişim sisteminden (sanal ortam) oluştuğu söylenebilmektedir.[478] Ülkemizde ise Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yayımlanan 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi' nde ise "siber uzay", *"Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamı"*[479] ifade eder şeklinde tanımlanmıştır. Kanaatimizce siber ve bilişim kavramlarının sıklıkla birbirleri yerine kullanılmakla birlikte "siber uzay" veya "siber ortam" kavramı ile "bilişim alanı" kavramı arasında da belirgin bir farklılık bulunmasa da belirtmek gerekir ki siber güvenliğin uygulama alanı olması ve uluslararası literatürde kullanımının daha yaygın olması karşısında bu kullanıma uygunluk oluşturması açısından çalışmamızın sistematiği de göz önünde bulundurulduğunda siber güvenliğe ilişkin hususlarda siber uzay terimini, hukuk sistemimiz içerinde yer alan bireysel bilişim suçları açısından ise hukuk sistematiğimizde de kullanımının bu yönde tercih edildiği "bilişim" veya "bilişim alanı" kavramlarını kullanacağız. Zira, teknolojinin hızla ilerlediği ve hızlı değişimlerin gerçekleştiği, sınırları olmayan bu alanda karşılaşılan siber sorunların tespiti ve çözümcü yaklaşımlar getirilebilmesi için anlaşmanın temeli olan ortak bir dil kullanımının zorunlu olduğunu düşünmekteyiz.

475 Güzin Ulutaş, "Siber Güvenlik", *Siber Güvenlik ve Savunma : Farkındalık ve Caydırıcılık*, Ed.: Şeref Sağıroğlu, Mustafa Alkan, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Ankara, Grafiker Yayınları, 2018, ss. 87- 101, s. 87.

476 European Commission, "Glossary and Acronyms", 2013, http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c 22 Şubat 2013 (*Aktaran* Hasan Çiftçi, *Her Yönüyle Siber Savaş*, 2. Bs., Ankara, Tübitak Popüler Bilim Kitapları, Salmat Basım Yayımcılık, 2017, s. 4).

477 Nato, "Cyber Definitions", 2015, http://ccdcoe.org/cyber-definitions.html 29 Temmuz 2015 (*Aktaran* Hasan Çiftçi, a.g.e., s. 4).

478 Çakmak ve Demir, a.g.e., s. 27, 28.

479 T.C. ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s. 7, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, ET. 02 Şubat 2020.

Bilgi ve iletişim teknolojilerinin sunmuş olduğu dijital teknolojilerden yararlanarak dijital bir altyapının oluşturulması yaklaşımının[480] benimsendiği günümüzde savunma sistemleri, enerji sektörü, ulaşım sektörü finans ve bankacılık alanı, telekomünikasyon alanı ve benzeri birçok sektörde sistemlerin işleyişi elektronik olarak kontrol edilir hale gelmiştir. Her yeni teknolojik gelişme ile hayatımızın kolaylaştığını söylemek mümkün olmakla birlikte söz konusu yenilikler beraberinde güvenlik riskini de beraberinde taşımaktadır. Başka bir anlatımla, bilgi ve iletişim sistemlerinin kamu kurumlarında, özel sektörde ve vatandaşlara ilave olarak; enerji, su kaynakları, sağlık, ulaşım, haberleşme ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlarda da kullanımının yaygınlaştığı günümüzde bilgi ve iletişim teknolojileri ve özellikle açık ve bağlantılı bir ortama erişilebilirlik sağlayan artan oranda internet kullanımı, siber uzaydaki tüm bileşenlerin birbiriyle bağlantılı olması ve siber uzayın bilişim sistemlerine ve bilgi/veriye yapılan saldırılar için anonimlik ve inkâr edilebilirlik gibi fırsatları sunması gerçeği siber güvenlik risklerini ve belirsizlikleri beraberinde getirmektedir.[481] Öyle ki bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve ulusal güvenliğin ihlaline neden olabileceği gibi siber saldırılar dolayısı ile olağanüstü boyutlara ulaşabilen maddi zararlar oluşabilmektedir.[482] Elektrik santrallerine yapılabilecek muhtemel bir saldırının bütün bir şehri ve hatta ülkeyi karanlık içinde bırakabilmesi, sanayi tesislerinin çalışamaz hale gelebilmesi, ulaşım ve haberleşme olanaklarının kullanılamaz hale getirilebilmesi gibi[483] birçok farklı risk ile karşı karşıya kalma ihtimalimiz bulunmaktadır. Siber ortamda etkin ve elverişli bir suç politikasının oluşturulabilmesinin sağlanabilmesi ve suçluluğun önlenebilmesi veya minimuma indirilebilmesi için ceza hukuku, polis hukuku, iletişim hukuku, güvenlik hukuku gibi çeşitli rejimler ve düzenleme modelleriyle ilişkili geniş kapsamlı hukuki önlemler, bu hukuki düzenlemelerin etkililiği için ise global siber uzayda bunların da ötesinde

480 Gerçek ve Gökşen, a.g.e., s. 25.
T.C. BİLİM, SANAYİ VE TEKNOLOJİ BAKANLIĞI, "Türkiye Dijital Yol Haritası (2018)" için bkz. https://cdnendustri40.4flyy.com/file/e267e931e0794d50b5e4ba40306cffcb/tsddtyh.pdf, ET. 2 Şubat 2020.
481 T.C. ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s, 5.
482 A.e.
483 Çakmak ve Demir, a.g.e., s. 29.

uluslararası işbirliği hukuku ve buna elverişli uluslararası araçlar, modern bilişim sistemlerinin teknik, organizasyonel ve personele ilişkin koruma önlemleri aracılığıyla güvenliğinin sağlanması ve farklı hukuk alanlarının birbirleriyle bağlantısı ve bu kurumların uyumlaştırılmış bir güvenlik tasarımı içindeki bağlantısını sağlayan geniş kapsamlı bir güvenlik hukukunun varlığı önem arz etmektedir.[484]

1.2.5.2. Siber Güvenlik

Ulusal ve uluslararası çerçevede yeni ve bir o kadar da karmaşık olan ve beşinci boyut olarak adlandırılan "siber uzay" boyutu kapsamında siber tehdit ve saldırıların yanında bilgi ve iletişim sistemleri (BİS) bünyesinde yer alan güvenlik açıklarını en aza indirmeyi amaçlayan ve bilginin korunmasını hedefleyen "siber güvenlik" kavramı öncelikli güvenlik alanlarından biri haline gelmiştir.[485] Siber saldırıların hedefinin merkezinde bilginin olması nedeniyle, başlangıçta 'Bilgi Güvenliği' olarak kullanılan kavramın siber güvenliği de kapsadığına dair yaklaşımların olmasına karşın, günümüzde siber ortamın hızlı değişimi dolayısıyla yaşanan olayların da etkisiyle bunun tersinin yaygınlaştığı, siber güvenliğin bilgi güvenliğini de içerir şekilde kullanılmaya başlandığı belirtilmektedir.[486] Siber güvenlik, siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitim ve teknolojiler bütünü olarak tanımlanmaktadır.[487] Veri, işlem, süreç, politika, deneyim, kapasite, insan ve sistemlerin güvenliğinin siber ortamda sağlanmasını ifade eden "siber güvenlik", Uluslararası Telekomünikasyon Birliği (ITU) tarafından "*kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü"* olarak tanımlamaktadır.[488]

484 H.C. Mult. Ulrich Sieber, *İnternetteki Suçlar ve Suçun İnternette Takibi : Global Bilgi Toplumundaki Yeni Gelişmelerin Işığında Hangi Önlemler Tavsiye Edilmektedir?,* Ed.: Yener Ünver, Çev.: Yener Ünver, Mustafa Temmuz Oğlakcıoğlu, Seçkin Yayıncılık, Ankara, 2014, s. 19, 20.

485 Ünal, a.g.e., s. 107, 111.

486 "Bu durum, "Konuyla ilgili farklı terimlerin ve tanımların ortak temalarından hareketle, siber güvenliğin devlet sırlarının korunması ve ulusal savunmanın sağlaması için temel esas olduğu…" şeklinde NATO Siber Güvenlik Çerçeve Kılavuzunda da açıkça vurgulanmıştır." Bkz. Şenol, a.g.e., s. 3.

487 Çiftçi, a.g.e., s. 8.

488 Şeref Sağıroğlu, "Siber Güvenlik ve Savunma, Önem, Tanımlar, Unsurlar ve Önlemler", *Siber Güvenlik ve Savunma : Farkındalık ve Caydırıcılık*, Ed.: Şeref Sağıroğlu, Mustafa Alkan, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, 1. bs., Grafiker Yayınları, Ankara, 2018, ss. 21- 45, s. 24.

Siber ortamın tehlikelerinin farkında olan ülkeler bu tehlikelerin siber güvenliğe karşı en önemli tehdit unsurlarından biri olarak kabul etmekte ve başta ülkenin elektronik haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans sektörleri vb. kritik altyapıları olmak üzere bireylerinin, kurum ve kuruluşlarının varlıklarını siber risklere, tehditlere ve saldırılara karşı korumak için çözümler üreterek uygulamaya koymaktadırlar.[489] Bu doğrultuda ülkemizde kabul edilmiş olan 2016-2019 Ulusal Siber Güvenlik Stratejisi' nde ise siber güvenlik:

> *"Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini"*[490], ulusal siber güvenlik ise: *"Ulusal siber uzayı oluşturan bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, bilgi/verinin ve bunların sunumunda yer alan donanım ve yazılım sistemlerinin ulusal ölçekte sağlanan siber güvenliğini"*[491] ifade eder şeklinde tanımlanmıştır.

Siber uzayda online alışveriş sistemleri, bankacılık sistemleri, elektrik-üretim ve dağıtım tesisleri, akıllı şebekeler, cep telefonu operatörleri, SCADA sistemleri, haberleşme sistemleri, doğal gaz kontrol ve aktarma sistemleri, hava trafik kontrol merkezleri, bilgisayar ve iletişim sistemleri, buna benzer kritik altyapılar ve ağlar, kritik yazılımlar ve buna benzer pek çok alanda yer alan uygulamalar ve sistemler bulunmakta ve bu ortamlara yapılacak saldırılar, ulusal hizmetlerin aksamasına, karmaşa, karışıklık veya kaosa sebebiyet verebileceğinden, siber güvenliğin sağlanması ulusal bir mesele haline gelmektedir.[492] Bunun yanında sanal para ve

489 Şenol, a.g.e., s. 3.
490 T.C. ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s. 8.
491 A.e.
492 Sağıroğlu, "Siber Güvenlik ve Savunma, Önem, Tanımlar, Unsurlar ve Önlemler", s. 37.
"Yüksek seviyede bir siber güvenliğin sağlanması ancak ve ancak aşağıdaki hususlara dikkat edilmesi ve bu unsurların yerine getirilmesiyle sağlanır. Bunlar; gizlilik, bütünlük, kimlik doğrulama, erişilebilirlik, inkar edememe gibi unsurlardır." Bkz. A.e., s. 41, 42.

blockzinciri[493], yapay zeka, nesnelerin interneti, "büyük veri"[494], derin öğrenme, kuantum çözümler[495] gibi yeni yaklaşımların, teknolojilerin, bakış açılarının ve uygulamalarının hızla artış gösterdiği günümüzde yeni tehdit ve tehlikelerin oluşacağı dikkate alındığında, siber güvenliğe ve savunmaya daha fazla ihtiyaç duyulacağı için önemlidir.[496] Zira her yeni teknoloji ile saldırganlar bu teknolojilerin açıklarını kullanarak güvenliği tehdit etmektedir. Bu anlamda, gelişen teknoloji ile kendilerini ve saldırı yöntemlerini de değiştiren ve geliştiren siber saldırılara karşı mümkün olduğunca ideale ulaşmaya çalışmak, siber güvenlik çözümünde ise sadece saldırıları

493 Satoshi Nakamoto tarafından geliştirilmiş olan Bitcoin (BTC), 2008'de hayatımıza giren, hiçbir finans kurumunun yönetmediği, P2P protokolü nü kullanan ve merkezi olmayan dijitalleşen dünyada değişimin ve dönüşümün önemli aktörlerinden birisi olan bir sanal para olup BTC adresi sahiplerinin açıkça tanımlanmadığı göz önüne alındığında bu tür işlemlerin anonim olarak yürütülmesi, yasadışı faaliyetleri ve işlemleri cezbetmesi, yasadışı işlemler için bir araç olarak kabul edilmesi, son dönemde fidye yazılımı mağdurlarının sayısının dünyada yüzbinlere çıkması, ulusal olduğu kadar işin uluslararası boyutunun olması, düzenleyici kurumlar ve yetkililerin yerinde uyarılar yapmasının haricinde henüz çözümler üretilmemesi veya üretmeye başlamamaları ülkelerde karşılaşılan temel sorunları oluşturduğu belirtilmektedir. Yine yapılan işlemleri P2P protokolü ile birbirine bağlı bilgisayarlar üzerinde blokzinciri yapısında tutmakta olan sanal paralardan bugün için borsada işlem gören 1500'e yakın farklı sanal paranın bulunduğu, ülkemizde bu alanda oluşabilecek suçları ve suçluları tespit edebilmek adına, EGM Siber Terörle Mücadele Daire Başkanlığının konuya önem vererek oluşabilecek tehdit ve tehlikeleri anlama, algılama ve önleme adına çalışmalar yaptıkları, 2018 yılında düzenlenen IBIGDELFT 2018 Konferansında konuya ilişkin sunumlar yapıldığı belirtilmekte, BTC ve blok zinciri teknolojileri yaygınlaştıkça, sıfırgün saldırılarının arttığı, güvenlik açığı sömürüsünün çoğaldığı, hizmet reddinin yanı sıra küçük blokzinciri sistemlerine yönelik saldırılarda artış olduğu, bu teknolojilerin hem bir tehdit hem de bir tehlike oluşturma potansiyeli olan teknolojiler olduğunun farkında olunmasının gerekliliği vurgulanmaktadır. Bkz. Sağıroğlu, "Siber Güvenlik ve Ötesi", s. 48- 50.

494 "Sosyal ağlar, toplumsal örgütlenme için de önemli bir altyapı sunmaktadır. Dernekler, vakıflar ve siyasal partiler tarafından yaygın olarak kullanılmaktadır. Toplumsal hareketler sosyal medya aracılığı ile organize edilmekte ve büyük toplulukları çeşitli aktiviteler için çok hızlı bir araya getirebilmektedir. Sosyal medya demek, büyük veri (big data) demektir. Sosyal medya, büyük veri için dünyanın en önemli kaynaklarından biridir. Dünyadaki mevcut verilerin %90'ı son iki yılda toplanmıştır. Bu verilerin %80'i sosyal medya kaynaklarından gelmektedir. Birçok sosyal medya şirketi ve devletler için büyük veriler çok değerli bir varlıktır ve bu veriler üzerinden yapılan analizler çok sayıda iş için büyük önem arz etmektedir." Bkz. Tacettin Köprülü, "Cumhurbaşkanlığı "Bilgi ve İletişim Güvenliği Tedbirleri" Genelgesi' ne İlişkin Değerlendirme", *CyberMag*, Sayı: 44, Eylül 2019, s. 19.

495 "Geliştirme aşamasında olan bu teknolojinin daha tam geliştirilmeden ve kullanıma açılmadan tehditleri olduğu da "kuantum teknolojisi ve yapay zeka gelecek için tehdit" isimli ABD İstihbarat Topluluğu Raporunda 2018 yılı sonunda yayımlanmıştır. Raporda; kuantum teknolojisinin ulusal güvenlik için yeni bir tehdit olduğu, bu teknoloji ile haberleşme sistemlerinin kolayca deşifre edileceği, önlem almanın zor olacağı, ilk hedeflerin ise ABD hükümeti ve askeri operasyonları olacağı belirtilmiştir. Ayrıca raporda; şifreleme sistemleri, otonom ve insansız araçlar ve teknolojilerine zarar vereceği öngörüldüğünden, en üst düzeyde endişe edilen teknoloji listesine alınmıştır.

Genel olarak değerlendirdiğimizde ise gelecek için önemli teknolojik gelişmelerin önünü açacak olan kuantum hesaplama teknolojilerinin; sektörün ve kurumların gelişmesine büyük katkı sağlayacağı fakat beraberinde de büyük endişeleri ve korkuları getireceği de muhakkaktır. Dolayısıyla, geliştirilen bu teknolojilerin siber güvenliğe ve savunmaya bakış açımızı kökten değiştirebilecek yaklaşımlar içerisinde olacağı hem daha hızlı, kaliteli ve güvenli sistemlerin ve uygulamaların geliştirilmesi hem de mevcut sistemlerin tehdit ve tehlike altında kalacağı unutulmadan çalışmalar yürütülmelidir." Bkz. Sağıroğlu, "Siber Güvenlik ve Ötesi", s. 56.

496 Sağıroğlu, "Siber Güvenlik ve Savunma, Önem, Tanımlar, Unsurlar ve Önlemler", s. 41, 42.

engellemekle kalmayıp saldırı ile karşılaşıldığı anda atılacak adımların ve sonrasında zararı telafi etmek için yapılacakların planlandığı bir sistemin varlığı için çalışılması gerektiği belirtilmektedir.[497]

Klimburg' a göre, ulusal siber güvenliğin sağlanmasında dikkate alınması gereken beş alan bulunmakta olup siber güvenlik stratejilerinde temas edilen ilk alan ülkenin sahip olduğu bilişim altyapısının korunmasına yönelik siber savunma olarak da ifade edilebilen askeri siber operasyonlar olup bunun da CERT tarzı, acil durumlara hızlı müdahaleye imkân sağlayan bir organizasyonel yapı gerektirdiği, ikinci alanın siber suçlarla mücadele edilmesi konusu olduğu bu kapsamda ulusal ve uluslararası hukuki altyapının oluşturulmasının gerekliliği, siber suçların özelliği nedeniyle uluslararası alanda işbirliği mekanizmaları geliştirmeye çaba göstermesi gerektiği, mücadelede dijital soruşturma becerilerini geliştirebilmiş adli bilişim alanında uzmanlaşmış polis birimlerine ihtiyaç duyulduğu, yine sınır aşan suçların soruşturulabilmesi için yabancı ülke polis teşkilatlarıyla ikili ilişkiler kurulmasının alanda ihtiyaç duyulan hız ve esnekliği sağlayacağı, siber suçlarla mücadelenin diğer bir boyutunu oluşturan da ticari kurumlardan bilişim suçları açısından en önemlilerinden birisi olan servis sağlayıcıların sunucularına yönelen e-posta trafiğini süzerek kullanıcılara daha az istenmeyen e-posta (spam e-mail) gitmesini sağlayabileceği, domain hosting (internet sayfalarının belli bir kira karşılığında barındırılması ve yayınlanması hizmeti) firmaları içerikleri üzerinde yapacakları denetimlerle siber suçlarla mücadele faaliyetlerine katılabilecekleri, sivil toplum kuruluşlarının da kullanıcıların bilişim sistemlerini kullanırken daha bilinçli davranmasına katkı sağlayabileceği, üçüncü alanın ulusal siber güvenliğin temellerinden birisi olan siber alanda istihbarat operasyonları yapabilme ve bu tür operasyonlara karşı koyabilme becerisi olduğu, dördüncü alanın siber güvenlik kriz yönetimi ve kritik altyapıların korunması bağlamında ulusal CERT (Computer Emergency Response Team) birimlerinin varlığı, bu birimlerin gelişen tehditlere yönelik olarak eğitimli olmaları ve güvenlik birimleriyle işbirliği yapmaları gerektiği bunun yanında kritik altyapılara yönelik standartlar geliştirilerek gerekirse kanunlar aracılığıyla özel ve kamuya ait kritik altyapıların bu standartlara kavuşturulması gerekliliği, beşinci ve son alanın ise siber diplomasi ve kuruluşundan bu yana herhangi bir devletin veya özel kuruluşun doğrudan etkisi altına girmemiş ve merkezi bir yapısı

497 CYBERMAG, "CISCO Orta Doğu ve Afrika Siber Güvenlik Direktörü Fady Younes İle Söyleşi", Sayı: 45, Ekim, 2019, s. 13, ss. 6-15.

olmayan internet ve internete yön veren politika ve standartların olduğu, interneti daha güvenilir bir hâle getirmek içinse şirketler ve bağımsız kuruluşlarca güvenli iletişim protokollerinin ve standart işlemlerin geliştirilmesi yönünde yapılan bu çalışmalara ulusal güvenlik bakımından katkı yapmak ve gelişmelerin dışında kalmamak gerektiği vurgulanmıştır.[498]

Bilişim sistemleri hızla gelişmekte ve kamu kurumlarına ilave olarak enerji, haberleşme, su kaynakları, tarım, sağlık, ulaşım, eğitim ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlarda da yoğun olarak kullanılmakta olup zaman içerisinde oluşturduğu riskler nedeniyle siber güvenliğin sağlanması için stratejiler belirlemeyi gerektirmiştir.[499] Siber Güvenlik konusu özellikle 2008 yılından itibaren AB (Avrupa Birliği), OECD (Ekonomik Kalkınma ve İşbirliği Örgütü/ Teşkilatı), NATO (Kuzey Atlantik Antlaşması Örgütü/ İttifakı) gibi uluslararası kuruluşlara ilave olarak tüm gelişmiş ülkelerin gündemine girmiş[500], Avrupa Birliği (AB) tarafından kurulan Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA-European Network and Information Security Agency)'nın Mayıs 2012'de yayınladığı Ulusal Siber Güvenlik Stratejileri raporuyla tavsiyelerde bulunulmuş olup siber güvenliğin sağlanmasının, hem ulusal hem de uluslararası düzeyde devletin, iş dünyasının ve toplumun ortak sorunu haline geldiğini belirten raporda AB'ye, AB'ye üye olan ve üye olmayan ülkelere ulusal siber güvenlik stratejilerini belirlemelerini tavsiye etmiştir.[501] AB, 07/02/2013 tarihinde siber güvenlik stratejisini belirlemiş ve

498 Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, 4 (2), 2013, ss. 135-158, s. 153, 154.

499 Kara, a.g.e., s. 2.

500 T.C. ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s, 7.

"Bilgi Güvenliği Derneğince Bilgi Teknolojileri ve İletişim Kurumu'nda (BTK) düzenlenen 12. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nda NATO Siber Güvenlik Mükemmeliyet Merkezi Direktörü Jaak Tarien: "Siber güvenlik, özellikle ordu, akademi ve özel sektör uzmanlarının birlikte çalışmasını gerektiren bir alan", "Siber güvenliğin özellikle 2007 yılında Estonya'nın uğradığı siber saldırıdan sonra uluslararası alanda daha fazla önemsenmeye başlandığını dile getiren Tarien, NATO üyeleri için bunun bir siber farkındalığa dönüştüğünü söyledi. NATO partnerlerinin 12 yıl önceki siber saldırıdan sonra siber güvenliğe üst düzeyde dikkat ettiğini belirten Tarien, "2007'de Estonya siber güvenlik alanında büyük bir saldırıya uğradı ve NATO'ya 'saldırıya uğradık.' diye ilettik fakat ortada ne tanklar ne de uçaklar vardı, görünen bir saldırı yok gibiydi. Bu tecrübeden sonra 2010 yılında siber güvenlik bir ulusal güvenlik tehdidi olarak NATO tarafından tanındı." şeklinde konuştu." Bkz. CYBERMAG, "12. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", 16.10.2019, https://www.cybermagonline.com/12-uluslararasi-bilgi-guvenligi-ve-kriptoloji-konferansi, ET. 23 Ekim 2019.

"2008'de NATO Siber Savunma Politikası hazırlanmış ve netice olarak 2009'da ise «Rapid Reaction Teams» kurulmuştur. Son olarak, daha önce de belirtildiği üzere 2016 Varşova zirvesinde ise siber uzayın da bir savaş alanı olarak tanımlanmasına karar verilmiştir." Bkz. Çelik, a.g.e., s. 117.

501 Kara, a.g.e., s. 2.

aynı tarihte Avrupa Komisyonu, birlik genelinde ortak bir ağ ve bilgi güvenliğinin ("NIS"[502]-Network and Information Security) sağlanmasına ilişkin tedbirlere dair direktif teklifi yayınlamıştır.[503]

Ülkemizde ise 2012/3842 sayılı Bakanlar Kurulu Kararı ile 11/6/2012 tarihinde Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar'ın yürürlüğe konulması kararlaştırılarak Ulaştırma ve Altyapı Bakanlığı' na (mülga Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na) siber güvenlik ile ilgili politika belirleme ve eylem planları hazırlama yetkisi verilmiş, 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı uyarınca mülga Telekomünikasyon İletişim Başkanlığı (TİB) tarafından siber güvenlik ile ilgili tehdit ve alınacak önlemlere ilişkin ulusal ve uluslararası çalışmalar yapmak için Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) kurulmuş, yine 2014 yılında 5809 sayılı Elektronik Haberleşme Kanunu'na 6 Şubat 2014 tarih ve 6518 sayılı Kanun'un 106. m.' siyle eklenen Ek 1. m. ile kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuş ve Kurula siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak, kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak, siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirleme görev ve yetkileri verilmiştir.[504] Türkiye'de siber güvenliğin sağlanması amacıyla en temel ve güncel belge niteliğinde olan 2016-2019 Ulusal Siber Güvenlik Stratejisi mülga Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yayınlanmış olup ulusal siber güvenliğin sağlanmasına belge oluşturacak nitelikte olan 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı Hazırlık Çalıştayı ise 19 Şubat 2020 tarihinde Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde

502 "NIS Direktifi nedir?
NIS Direktifi (2016/1148) siber güvenlik alanında AB genelini kapsayan ilk yasal düzenlemedir. AB'deki genel siber güvenlik düzeyini arttırmaya dönük yasal tedbirleri içerir. 6 Temmuz 2016 tarihinde Avrupa Parlamentosu tarafından kabul edilerek Ağustos 2016'da yürürlüğe girmiştir. Üye Devletlerin büyük çoğunluğunda ulusal mevzuata aktarım süreci tamamlanmıştır." Bkz. AVRUPA BİRLİĞİ TÜRKİYE DELEGASYONU, "AB Türkiye'de Şebeke ve Bilgi Sistemleri Güvenliğini Destekliyor", 11.04.2019, https://www.avrupa.info.tr/tr/pr/ab-turkiyede-sebeke-ve-bilgi-sistemleri-guvenligini-destekliyor-9420, ET. 20 Mart 2020.
503 A.e.
504 Mehmet Bedii Kaya, "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik, Adli Bilişim ve Güncel Teknolojiler", *Siber Güvenlik ve Savunma : Problemler ve Çözümler*, , Ed.: Şeref Sağıroğlu, Mustafa Şenol, BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Ankara, Grafiker Yayınları, 2019, ss. 213-269, s. 255-258.

gerçekleştirilmiştir.[505] Bunun yanında 2016 yılında 671 sayılı Kanun Hükmünde Kararname'nin 25. m.' siyle Elektronik Haberleşme Kanunu'nun 60. m.' sine eklenen onuncu fıkra ile Bilgi Teknolojileri ve İletişim Kurumu'na (BTK), kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma veya aldırma yetkisi tanınmış, Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği'nde 2018 yılında yapılan değişiklikle de *"Ulusal siber güvenlik faaliyetleri ile siber saldırılara karşı korunma ve caydırıcılığın sağlanmasına yönelik Kurumun görevleri kapsamında belirleyeceği yükümlülükleri yerine getirmeyen veya aldıracağı tedbirleri uygulamayan gerçek kişiler ile işletmeciler dışındaki özel hukuk tüzel kişilerine bin liradan bir milyon liraya kadar idarî para cezası"* uygulanacağı hükme bağlanmıştır.[506] Belirtmiş olduğumuz düzenlemelerin ülkemizde siber güvenliğin açık yasal dayanağını oluşturmaları açısından önemli olduğu bu düzenlemeler müstakil bir Siber Güvenlik Yasası yürürlüğe konuluncaya kadar boşluğu doldurması açısından önem arz ettiği belirtilmektedir.[507]

Ülkemizin siber güvenlik konusunda izleyeceği yolu belirleyen ve siber güvenliğin sağlanması amacıyla en temel ve güncel belge niteliğinde olan 2016 - 2019 Ulusal Siber Güvelik Strateji ve Eylem Planı'nda, siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve

505 Bkz. BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, "2020-2023 Siber Güvenlik Stratejileri BTK'da Belirlendi", 10.02.2020, https://www.btk.gov.tr/haberler/2020-2023-siber-guvenlik-stratejileri-btk-da-belirlendi, ET. 20 Şubat 2020.

506 A.e.

"Ulusal Siber Olaylara Müdahale Merkezi'ne (USOM) siber güvenlikle ilgili gerekli tedbirleri almayan firmalara yönelik bin liradan 1 milyon liraya kadar para cezası verme yetkisi verildi.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) İdari Yaptırımlar Yönetmeliğinde yapılan değişiklikle yasal dayanağı da bulunan ulusal siber güvenlikle ilgili yaptırımlar tanımlandı. Yapılan düzenlemeyle siber güvenlik alanında önemli ölçüde caydırıcılık sağlanacak.

Firmaların hizmet olarak sunduğu altyapılarda, sistemlerde, yazılım ve donanımlarında zafiyet bulunması ve bildirilen önlemleri almamaları durumunda BTK bünyesinde bulunan USOM tarafından para cezası verilebilecek.

Son bir yılda 6 bin zafiyet tespit edildi

Son dönemde, siber saldırıları tespit ve önleme kapasitesi teknik imkanlarla üst düzeye çıkarıldı. USOM'un yerli olarak geliştirdiği AVCI, AZAD ve KASIRGA altyapılarıyla sürekli olarak ülke genelindeki sistemler saldırılara karşı izleniyor.

Geçen yıllarda WannaCry ve Petya gibi dünya genelinde birçok ülkeyi vuran siber saldırıların kullandığı zafiyetler önceden tespit edilerek operatörler ve yer sağlayıcı (hosting) firmalara bildirildi ve bu sayede Türkiye'de saldırıların etkisi hissedilmedi." Bkz. ANADOLU AJANSI, "USOM'a idari para cezası kesme yetkisi verildi", 30.09.2018, https://www.aa.com.tr/tr/turkiye/usoma-idari-para-cezasi-kesme-yetkisi-verildi-/1268694, ET. 26 Ekim 2019.

507 Ülkemizdeki siber güvenlik faaliyetleri hakkında ayrıntılı bilgi için bkz. Çiftçi, a.g.e., s. 397-427.

teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılması amacıyla, 5 ana eylem ve 41 alt eylemin gerçekleştirilmesi öngörülmüş ve Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması, Siber Suçlarla Mücadele, Farkındalık ve İnsan Kaynağı Geliştirme, Siber Güvenlik Ekosisteminin Geliştirilmesi, Siber Güvenliğin Milli Güvenliğe Entegrasyonu başlıklı siber güvenlik yol haritasını oluşturan ana eylem maddeleri belirlenmiştir.[508]

508 Şenol, a.g.e., s. 6.

2016-2019 Ulusal Siber Güvenlik Stratejisi' nde mevcut riskleri, belirlenen ilkeler ışığında asgari düzeye indirmeyi hedefleyen stratejik amaçlar:

"1. Ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar (Ek-B) tarafından denetlenmesi,

2. Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması,

3. Sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi,

4. Kurumların bilişim sistemlerinin sadece saldırılardan değil, kullanıcı hataları ve afetlerden de korunması için düzenlemelerin yapılması,

5. Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması,

6. Siber güvenlik konusunda kurum yöneticilerinin farkındalığının artırılması,

7. Siber güvenlik alanında yetkin personel yetiştirilmesi ve bu alanda uzmanlaşmak isteyen personel, araştırmacı ve öğrencilerin teşvik edilmesi,

8. Toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması,

9. Kamu kurumlarında siber güvenlik alanında uzman personel istihdam edilmesi için mevzuat desteği sağlanması ve personelin özlük haklarının iyileştirilmesi,

10. Kurumsal ve Sektörel SOME'lerin (Siber Olaylara Müdahale Ekibi) (Ek-C) etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, yetkin personel ihtiyacının karşılanması, bilişim altyapısının sağlanması ve ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımının geliştirilmesi,

11. Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması,

12. Kamu kurumları, özel sektör, STK'lar (Sivil Toplum Kuruluşu), denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyon hedefi ile ulusal siber güvenlik eko-sisteminin oluşturulması,

13. Ulusal Siber güvenlik eko-sistemi içinde iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması,

14. Bilişim sistemlerinin kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin içerdiği açıklıkların kötüye kullanılmasına engel olmak üzere açıklık analizi ve sertifikasyon çalışmalarının yapılması,

15. Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması,

16. Siber güvenlikte dışa bağımlılığı azaltmak için Ar-Ge faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi,

17. Tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi,

18. Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliği ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılması"

olarak belirlenmiştir. Bkz. T.C. ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s, 13, 14.

1.2.5.3. Siber Saldırı, Siber Saldırı Türleri ve Kullanılan Kötü Amaçlı Yazılım Çeşitleri

Teknolojinin sağlamış olduğu fayda ve olanaklarla ortaya çıkan çevirim içi kullanıcı sayısı ve toplam veri büyüklüğünün hızlı artışı özellikle internet tabanlı uygulama ve hizmetler kötü niyetli kişilerin siber saldırılarına kalma riskini ve güvenlik tehditlerini de beraberinde taşıyor, uzaktan ve çok hızlı bir şekilde hareket edebilen siber saldırganlar fidye virüsü, zararlı yazılım, kimlik avı vb. yöntemlerle kullanıcıların sistemlerine yetkisiz erişim sağlanarak veriler ele geçirilebiliyor ya da tahrip edilebiliyor, bir ağa izinsiz giriş yaparak uzun süre fark edilmeden kalabilen gizli bilgisayar ağ saldırıları da özellikle devlet kurumlarını politik nedenlerle hedef alabiliyor.[509] Bu kapsamda çalışmamızın bu başlığı altında siber saldırı kavramı ve siber saldırı türleri incelenerek bu zamana kadar gerçekleşmiş siber saldırılara örnekler verilecek, ülkelerin siber saldırılara karşı aldıkları önlemlere ve siber güvenlik alanında yapmış olduğu çalışmalara değinilecektir.

1.2.5.3.1. Siber Saldırı

Siber uzayda, kişilerden büyük çaptaki organizasyonlara, terör örgütlerinden devletlere kadar çeşitli kaynaklar tarafından hedef alınan sistemlerin bozulması veya kullanılamaz hale getirilmesine yönelik saldırılar gerçekleştirilebilmektedir.[510] ABD Ulusal Araştırma Konseyi tarafından, 2009 yılında yapılan bir çalışmada siber saldırı, *'Bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler'*[511] olarak tanımlanmıştır. 2016-2019 Ulusal Siber Güvenlik Stratejisi Belgesi' nde ise "siber saldırı", "*Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/ veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemleri"*[512] ifade eder şeklinde tanımlanmaktadır.

509 BASIN İLAN KURUMU, "Teknolojiyle kapıyı çalan tehlike: Siber Saldırı" Editör: Ömer Faruk Orkçu, 16.03.2019, https://www.bik.gov.tr/teknolojiyle-kapiyi-calan-tehlike-siber-saldiri/, ET. 18 Şubat 2020.
510 Çiftçi, a.g.e., s. 6.
511 P.W., Singer, A., Friedman, Siber Güvenlik ve Savaş, Buzdağı Yayınları, Ankara, 2015 (*Aktaran* Şenol, a.g.e., s. 2).
512 T.C. ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s, 8, 9.

Bir saldırının "siber saldırı" olabilmesi için saldırıların siber ortam kullanılarak yapılması gerekmektedir.[513] Siber saldırıların verilere veya kontrol sistemlerine yönelik olarak iki temel şekilde meydana geldiği, bilginin çalınması veya bozulmasının sıklıkla karşılaşılan verilere yönelik eylemlerden, kontrol sistemleriyle ilgili olanların ise fiziksel bir altyapıyı kullanılamaz hale getirme veya manipüle etmeyi kapsadığı belirtilmektedir.[514]

2000'de Avustralya'da arıtma tesisi bilgi sistemlerine saldırı ve kanalizasyon sularının şehre bırakılması, 2003'te ABD'nin 8 eyaletinde 2 gün süren, ölümlere ve 6 milyar dolar zarara yol açan elektrik kesintisi, 2007'de Rus bilgisayar korsanlarının Estonya bilgi sistemlerine saldırısı ve ülke çapında faaliyetlerini durma noktasına getirmesi, 2010'da İran nükleer zenginleştirme programını hedefleyen ve büyük sorunlara sebep olan 'Stuxnet' yazılımı saldırısı, 2010'da "WikiLeaks"[515] in yayınladığı belgeler ile diplomaside sanal bomba etkisi yaratması, 2011'de İran Silahlı Kuvvetlerinin ABD'ye ait insansız hava aracının kontrolünü ele geçirerek yere indirmesi, 2016'da ABD'nin doğu yakasına hizmet sunan sistem altyapılarına yönelik olarak başlayan siber saldırıların ülke geneline yayılarak internet bağlantısını engellemesi ve ciddi ekonomik zarara sebep olması, Türkiye' de ise 2008'de Bakü-Tiflis-Ceyhan boru hattına yapılan siber saldırı sonrası meydana gelen patlama, 2009'da zararlı bir yazılım sonucunda Atatürk Havalimanı bilgisayarlarının etkilenmesi, 2015'te elektriğini İran'dan alan Van ve Hakkâri hariç 79 ili etkileyen elektrik kesintisi, 2015'te, 10 gün süreli saldırılar sonucu birçok banka, noter ve devlet kurumunun internet sitesine ve mobil uygulamalara erişim sağlanamaması, 2016'da Sağlık Bakanlığı hastanelerine yönelik siber saldırılar sonucunda veri tabanındaki bilgilerin çalınması ve silinmesi örnekleri çeşitli amaçlarla gerçekleştirilen farklı tip

513 Çiftçi, a.g.e., s. 6.
"… siber saldırılar aşağıdaki gibi sınıflandırılabilir:
· Elektronik posta eklentileriyle virüs saldırıları,
· Kamu hizmetlerinin görülmesini sağlayan bilgisayar sistemlerinin aşırı yüklenmesini sağlayarak çalışamaz hale getirilmesi (hizmetin engellenmesi),
· Dezenformasyon ya da propaganda yapmak maksadıyla devletlerin veya ticari kuruluşların internet sayfalarının bozulması,
· Bilgisayar sistemlerine yetkisiz girişler yapılarak kişisel bilgilerin elde edilmesi." Bkz. Çakmak ve Demir, a.g.e., s. 30.
514 A.e.
515 "Wikileaks CIA Vault 7: Mart 7'de, WikiLeaks CIA'den çalınmış 8761 adet dökümanın bulunduğu bir veri ambarı yayınladı. Bu ambarda birçok hacking aracı ve spying işlemlerinin dökümantasyonu mevcuttu. IOS ve Android zafiyetleri, Windows'daki böcekler, bazı akıllı TV'leri dinleme cihazına dönüştürebilme yöntemleri ile alakalı dökümanlar bu ambarda mevcuttu. Wikileaks bu ambarı "Vault 7" olarak adlandırdı." Bkz. Ulutaş, a.g.e., s. 96.

ve büyüklükteki siber saldırılarla siber savaşların başlayıp devam ettiği çağımız dünyasında, internet medyası ile yazılı ve görsel basın gibi açık kaynaklara da yansıyan önemli siber saldırılardan bazılarını oluşturmaktadır.[516] Güncel bir örnek vermek gerekirse dünya çapındaki en geniş kapsamlı siber saldırılardan biri olan "WannaCry"[517] saldırısı tüm dünyada çok sayıda bilgisayar kullanıcısını, kritik önem taşıyan sistemi ve 150 ülkede 230 binden fazla bilgisayarı etkiledi.[518] Yine ülkemizde güncel olarak 27 Ekim 2019 günü gün boyunca büyük kuruluşlara yapılan, "DDOS"[519] (Distributed Denial of Service- Dağıtık Hizmeti Engelleme Saldırısı) adı verilen yöntemle gerçekleştirildiği tahmin edilen siber saldırı gerçekleştirildi ve bu saldırı internet erişiminde aksaklıklara neden oldu.[520]

516 Şenol, a.g.e., s. 3.

517 "Mayıs 2017'de WannaCry şifreleyicisi ile bir dizi saldırı gerçekleştirildi.WannaCry halen tarihin en büyük fidye yazılımı salgınlarından biri olarak kabul ediliyor. Saldırıların başlamasından 2 ay önce, EternalBlue 2'nin yararlandığı açığı kapatmak için Windows işletim sistemine bir yama çıkarılmış olsa da WannaCry dünya genelinde yüz binlerce cihazı etkilemeyi başarmıştı. Diğer şifreleyicilerde olduğu gibi, WannaCry kurbanların bilgisayarlarındaki dosyaları şifreli veriye dönüştürüp şifreleri çözecek anahtarlar (dosyaları çözüp orijinal hallerine dönüştürmek için saldırganlar tarafından hazırlanan) için fidye talep ediyordu. Fidye ödenmediğinde, saldırıya uğrayan cihazları kullanmak imkânsız oluyordu.
WannaCry salgınının sonuçları yıkıcı oldu. Bunun nedeni, kurbanların genellikle ağ üzerinden bağlı sistemlere sahip olan kurumlar olmasıydı. İşletmelerin, fabrikaların ve hastanelerin çalışmaları durdu. Şifreleyicilerin ne kadar tehlikeli olduğunu gösteren ve dünya genelinde birçok bilgisayarın EtenalBlue açığını kapatmak için güncellenmesini sağlayan bu olaya rağmen istatistikler, suçluların halen çok sayıdaki güncellenmemiş bilgisayara saldırmayı denediklerini gösteriyor." Bkz. CYBERMAG, "WannaCry 2018'in 3. Çeyreğinde Yaklaşık 75.000 Kullanıcıyı Etkiledi", Sayı: 36, Ocak 2019, ss. 42-43, s. 42.
"WannaCry: 12 Mayıs 2017'de WannaCry isimli bir fidye yazılımı tüm dünyaya yayıldı (150 den fazla ülkede 200.000 den fazla sistem bu durumdan etkilendi) [16, 17]. Genel kuruluşlardan büyük işletmelere kadar birçok birim bu zararlı yazılımın etkisinde kaldı. İngiltere'deki National Health Service hastaneleri ve tesisleri geçici olarak işlem dışı kaldı ve bu durum İngiliz sağlık sistemi için o anda önemli bir kaos oluşmasına sebep oldu. Rusya'da ilgili fidye yazılımından en çok etkilenen ülkeler arasında yer aldı. Kamuya bağlı demiryolu şirketleri, Rusya'nın en büyük ikinci Telekom ağı fidye yazılımından etkilenen önemli kurumlar arasında yerini aldı. İspanya, Almanya, Fransa, İsveç ve Amerika'da ilgili yazılımın etkisinde kalan ülkeler arasındaydı." Bkz. Ulutaş, a.g.e., s. 95.

518 "İspanyol telekomünikasyon şirketi Telefonica saldırıdan en çok etkilenen kurumlar arasında yer alıyor. İngiltere Ulusal Sağlık Hizmetleri'ne (NHS) bağlı bir çok kurum da saldırının kurbanı oldu. Renault'un Bursa fabrikası da dahil olmak üzere birçok tesisinde üretim durduruldu. Benzer şekilde Nissan'ın İngiltere'deki fabrikası da üretime ara vermek zorunda kaldı. PetroChina, Portugal Telecom, FedEx, Saudi Telecom, Deutsche Bahn da WannaCry kurbanı şirketler arasında.
Bunların yanı sıra Rusya Demiryolları, Rusya İçişleri Bakanlığı, Çin Halk Güvenliği Bürosu, Romanya Dışişleri Bakanlığı gibi devlet kurumları da WannaCry saldırısı altında kaldı." Bkz. CNNTURK, "WannaCry saldırısının ardında yatan gerçekler", 16.05.2017, https://www.cnnturk.com/teknoloji/wannacry-saldirisinin-ardinda-yatan-gercekler, ET. 9 Şubat 2020.

519 "Dağıtık Dos(DDoS), failin birden fazla benzersiz IP adresi kullandığı bir siber saldırıdır.(genellikle binlerce). DDoS saldırılarının ölçeği, 2016 yılına kadar saniyede bir terabiti aşarak son yıllarda artmaya devam etti." Bkz. https://tr.m.wikipedia.org/wiki/Denial-of-service_attack, ET. 20 Şubat 2010.

520 MİLLİYET, "Türkiye'ye siber saldırı şoku: Kaynağı ABD ve Rusya!", 30.10.2019, https://www.milliyet.com.tr/teknoloji/turkiyeye-siber-saldiri-soku-kaynagi-abd-ve-rusya-6066357, ET. 9 Şubat 2020.

Siber saldırılar sosyal ağlar, akıllı şebekeler, kapalı devre sistemler, acil yardım sistemleri, Web sayfalarını, kritik altyapıları hedef alabilmekte[521] bununla birlikte hacktivizm ve maddi kazanç elde etmek amaçlarıyla da gerçekleştirilebilmektedir.[522] Özellikle son dönemlerde artan saldırıların öncelikli hedefleri ise enerji santralleri, su depoları, bankalar, hastaneler, lojistik şirketleri, e-ticaret siteleri, bulut bilişim hizmet sağlayıcıları ve arama motorları olup bu durum bizleri, saldırganların kişisel verileri elde etmek için planlı hareket ettikleri sonucuna götürmektedir.[523] Yine hedeflerine medya cihazları dahil olmak üzere evlerdeki nesnelerin interneti cihazlarını ekleyen saldırganlar, bu cihazların sürekli internete bağlı olması sebebiyle sürekli olarak sistemin altını oymaya devam eden zararlı yazılımlar yükleyerek bu cihazlardan yararlanabiliyorlar[524], evlerde ve işyerlerinde daha fazla sayıda internet bağlantılı cihazların kullanılması ile bu cihazların kontrolünün ele geçirerek botnet ağlarının bir parçası haline geçirebilmektedirler.[525] Akıllı evlerin de saldırganların yeni hedeflerinden biri olduğu[526], mobil cihazları hedef alan zararlı yazılımların da yaygınlaştığı belirtilmektedir.[527] Yaklaşık 20 yıldır kullanılan ve güvenlik konusunda kötü şöhrete sahip olan USB cihazları ise siber saldırganların hedefinde olmaya devam ederken son birkaç yılda dikkate değer ölçüde istikrarlı olan bazı tehditleri yaymak için de kullanılıyor.[528] Rastgele saldırıların ise yerini planlanmış bir fidye yazılımı

521 Ayrıntılı bilgi için bkz. Ünal, a.g.e., s. 112-114.

522 Ayrıntılı bilgi için bkz. Kara, a.g.e., s. 16-27.
"Hacker ve activism kelimelerinin karışımı ile oluşturulmuş yeni bir terimdir. Hacktivist, amaçları için siber ortamı kullanmayı tercih eden, sanal protestoculardır." Bkz. a.e., s. 16.

523 CYBERMAG, "2018'in Siber Tehditlerini Tanımlayan Kelimeler: Gizli ve Daha Zeki", Sayı: 34, Kasım 2018, ss. 24-25, s. 25.
Nitekim, "2017'nin ikinci yarısından itibaren SCADA'daki (Veri Tabanlı Kontrol ve Gözetleme Sistemi) sorunlar artmaya devam etti. Bu sorunların büyük çoğunluğu da HMI (İnsan Makine Arayüzü) yazılımlarındaydı. SCADA HMI, kritik altyapıları yöneten ana bağlantı noktası olduğundan, saldırganlar için burada bulunan verinin değeri de çok cazipti." Bkz. A.e., s. 24.

524 CYBERMAG, "Firmalar En Az Bir Kez Ciddi Bir Siber Saldırıya Maruz Kalıyor", Sayı: 34, Kasım 2018, ss. 26-27, s. 26.

525 CYBERMAG, "Artık Milyonlarca Kişinin Değil, Milyonlarca Doların Peşine Düşüyorlar", Sayı: 36, Ocak 2019, ss. 30-31, s. 31.

526 "Ocak ayından bu yana her ay artan bir grafik gösteren siber saldırılar, özellikle Haziran'da 13 milyonun üstünde belirlenen saldırı sayısı ile zirve yaptı. Yapılan saldırıların yüzde 37'den fazlası, cihazların üretim aşamasında belirlenmiş şifrelerini elde ederek gerçekleştirilirken toplam saldırıların yüzde 30'a yakını da kripto para madenciliği amacı taşıyordu." Bkz. CYBERMAG, "Türkiye, Orta Doğu'da Siber Saldırıların Odağında", Sayı: 34, Kasım 2018, s. 33.

527 CYBERMAG, "Artık Milyonlarca Kişinin Değil, Milyonlarca Doların Peşine Düşüyorlar", Sayı: 36, Ocak 2019, ss. 30-31, s. 31.

528 CYBERMAG, "Her 10 Zararlı Yazılımdan Biri Kripto Para Madencisi", Sayı: 34, Kasım 2018, ss. 30-31, s. 30.
"USB cihazları 2018'de, 21 Ağustos 2018'de raporlanan ve en az 2013'ten beri Meksika'da tüketicileri ve kurumları etkileyen, bankacılık hedefli Dark Tequila adlı gelişmiş zararlı yazılımı yaymak için de kullanıldı. Ayrıca, KSN verilerine göre 2018'in ilk yarısında endüstriyel kontrol

olarak tanımlanabilecek saldırılara bıraktığı, siber saldırganların ödeme kartı verilerini, internet bankacılığı hesaplarını çalmak, ATM makinelerini bozmak için fidye yazılımları, kripto madenciliği ve diğer kötü amaçlı yazılımları kullanarak finansal hizmetler sektörünü hedef almaya devam ettiği de belirtilmektedir.[529] Son dönemlerde ise sosyal medya tabanlı siber saldırıların kurumları ve son kullanıcıları hedeflediği görülmektedir.[530] Günümüzde dijital veri kayıtlarının saklanması için bulut ortamına taşınan veriler de siber saldırıların tehdidi altında bulunmaktadır.[531]

Siber saldırılar sonucu oluşan siber suçlar ise çeşitli şekilde sınıflandırılabilmekte olup literatürde yer alan bazı sınıflandırma çeşidine göre siber suçları: kişilere yönelik siber saldırılar, mülkiyete yönelik siber saldırılar, kurumlara yönelik siber saldırılar oluşturmaktadır.[532] Symantec'in yayınladığı güvenlik raporuna göre 2016 yılında A.B.D.' de yaklaşık 791 milyon "kimlik hırsızlığı"[533] vakası meydana gelmiş olup sıralamada Amerika'yı Fransa ve Rusya takip etmektedir.[534]

---

sistemlerini hedef alan saldırıların %8'i çıkarılabilir medya cihazları üzerinden gerçekleştirildi." Bkz. A.e., s. 31.

529 CYBERMAG, "Finansal Hizmetler Sektörü Siber Suçluların Radarında", Sayı: 45, Ekim, 2019, ss. 24-27, s. 24, 25.

530 "…siber suçluların, sahte Twitter hesapları kullanarak gerçek satıcıların güvenilir teknik destek hesaplarının benzerlerini oluşturarak dolandırıcılık yaptıkları belirlendi. Kullanıcılar, hesaplardaki sahte telefon numaralarını arıyor ve gerçekte aramak istedikleri şirketin müşteri hizmetleriyle konuştuklarını düşünüyorlar. Ardından kredi kartı bilgilerini paylaşıyor ya da bilgisayarlarına bilmeden kötü amaçlı içeriği yüklüyorlar." Bkz. CYBERMAG, "Siber Tehditlerin Yeni Silahı: Sosyal Medya", Sayı: 45, Ekim 2019, ss. 34-35, s. 34.

531 "…Bulut ortamı, sağlık sektöründe büyük kolaylıklar sağlıyor olsa da geçiş sürecinde başlayan ve devamında da gerçekleşen hatalar, kuruluşlara ciddi zararlar veriyor…" bkz. CYBERMAG, "Son 10 Yılda 190 Milyon Sağlık Kuruluşu Verisi İfşa Edildi", Sayı: 45, Ekim, 2019, SS. 38-39, s. 38.

532 Mahmut Sami Öztürk, "Siber Saldırılar, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi", *Muhasebe ve Vergi Uygulamaları Dergisi*, Özel Sayı, Nisan 2018, ss. 208-232, s. 212.

533 "Kimlik Hırsızlığı: Kimlik hırsızlığı, genellikle bir siber hırsızın bir kişinin kimliğine ait bilgileri çaldığı durumda ortaya çıkmaktadır. Maddi bir karşılığı olmadığı sürece kimlik hırsızlığı bir getiri sağlamamaktadır. Dolayısıyla kimlik hırsızlığı; vergi iadesi dolandırıcılığı, kredi kartı sahtekârlığı, kredi dolandırıcılığı ve benzeri diğer suçlara bir kapı oluşturmaktadır. Hileli olarak bir kredi hesabı açılması, mal veya hizmet satın alınması, bir ev veya dairenin kiralanması veya satın alınması, tıbbi bakım alınması, istihdam sağlanması, trafik ihlallerinin veya suçların işlenmesi, açık artırma dolandırıcılığı ve ücretlerle ilgili dolandırıcılıklar kimlik hırsızlığına ait bazı örneklerdir." Bkz. A.e., s. 213.

534 "Steve Morgan tarafından Forbes'da yayınlanan bir makalede ise 2016 yılı için elde edilen istatistikler şu şekildedir:

· AT&T Siber Güvenlik Raporu'na göre, bilgisayar korsanlarının saldırıları sonucu, Nesnelerin İnterneti bağlantılarındaki güvenlik açığı sayısında %458 oranında artış meydana gelmiştir.

· Cisco Yıllık Güvenlik Raporu'na göre, internet sitelerinin güvenlik ihlallerinde %221 oranında artış meydana gelmiştir.

· Dell Yıllık Güvenlik Raporu'na göre, kötü amaçlı yazılım sayısı yaklaşık iki katına çıkarak yaklaşık 8 milyara ulaşmıştır.

· Google Android Güvenlik Raporu'na göre, günlük 6 milyardan fazla uygulama ve 400 milyondan fazla cihaz tehditlere karşı kontrol edilmektedir.

Dünyanın siber tehdit efsanelerini dikkate almasını sağlayan 2007 yılında Estonya'ya gerçekleştirilen siber saldırı, 2010 yılında Çin'de Google ve diğer sitelere yapılan Aurora kod adlı saldırılar, 2008'de Microsoft ürünlerini hedefleyen Conficker adındaki solucan, İran nükleer programını hedefleyen Stuxnet solucanı ve daha birçok yeni saldırı yöntemi ülkelerin kendi varlıklarını ve vatandaşlarının bilgi güvenliğini korumak için daha etkin teknik ve hukuksal önlemler almaları gerektiğini göstermiş, NATO, Birleşmiş Milletler, Avrupa Birliği, AGIT ve diğer birçok uluslararası örgütün güvenlik politikaları bu sayede revize edilmeye başlanmıştır.[535] Bu değişim sürecinde birtakım evrensel kurallar oluşmuştur: "bölgesellik kuralı"[536], "sorumluluk kuralı"[537], "işbirliği kuralı",[538] "öz-savunma kuralı"[539], "veri koruma kuralı"[540] , "bakım

· IBM X-Force Siber Güvenlik Endeksi Raporu'na göre, sağlık endüstrisi dünyada en hızlı siber saldırıya uğrayan sektördür. Bunu finansal hizmetler ve üretim sektörü takip etmektedir.

· McAfee Labs Tehdit Tahminleri Raporu'na göre, 2016 yılında otomobil sistemlerine yapılan siber saldırıların hızla artacağı öngörülmektedir.

· Symantec İnternet Güvenlik Tehdit Raporu'na göre çalışanları hedef alan kimlik hırsızlığı girişimleri geçen yıla göre %55 oranında artış göstermiştir.

· Verizon Veri İhlal Araştırma Raporu'na göre, bütün siber saldırıların %89'u finansal çıkar ve casusluk için yapılmaktadır." Bkz. Öztürk, a.g.e., s. 216.

535 Seda Yılmaz ve Şeref Sağıroğlu, "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", *ISC Turkey 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, Bildiriler El Kitabı, 20-21, Eylül 2013, Ankara, ss. 158-166, s. 159, https://vdocuments.mx/siber-guevenlik-risk-analizi-tehdit-ve-hazirlik-seviyeleri.html, ET. 11 Şubat 2020.

536 "Bir devletin toprakları içinde yer alan bilgi teknolojileri altyapısı devletin ulusal egemenlik unsurudur. Uluslar arası hukuk anlayışına göre; her devlet kendi ülkesinin bilgi teknoloji altyapısına karşı gerçekleştirilecek her türlü tehdit ve saldırıya karşı önlem almak ve bunlarla başa çıkabilmek için BT altyapısına yönelik her türlü iyileştirme yetkisine sahiptir." Bkz. a.e.

537 "Bir devletin topraklarında bulunan bilgi sistem kaynağına düzenlenen siber saldırıların başka bir ülke kaynaklı olduğu varsayımı oluştuğunda sorumlu tutulan ülkenin konu ile ilgili soruşturma yapması, suçluların yakalanmasına yardımcı olması ve yargılanma sürecini desteklemesi beklenir." Bkz. a.e.

538 "Siber saldırı, bir devletin topraklarında bulunan bilgi sistemleri aracılığıyla başka bir ülkeyi hedef alarak gerçekleştirilmiş ise saldırı kaynakları kendi topraklarında olan devletin kurban devlet ile işbirliği yapma görevi vardır. Uluslar arası Siber Suçlar Sözleşmesine göre, tarafların cezai konularda uluslar arası araçlar ile hukuk kurallarının uygulanmasını ve elektronik kanıtların toplanmasını talep etme hakları vardır. Bunun yanı sıra Kuzey Atlantik Antlaşması uyarınca herhangi bir ülkenin toprak bütünlüğünü, siyasi bağımsızlığını ve güvenliği tehdit eden bir durum oluşması halinde diğer taraf ve müttefik ülkelerin işbirliği yapması zorunludur." Bkz. a.e.

539 "Uluslar arası ceza kanunlarına göre kişiler, yasaların kişisel özgürlüklerine karşı yasadışı olarak kullanıldığını düşündüğünde kendini korumak amacıyla gerçekleştirebilecekleri haksız eylemlerden sorumlu tutulamaz. Uluslar arası düzeyde eğer bir ülke bireysel ya da toplu olarak gerçekleştirilen bir saldırının güvenliğini tehdit ettiğini düşünürse silahlı güç de dahil olmak üzere belirlediği bir yöntemle saldırılara cevap verme hakkına sahiptir. Hatta NATO anlaşmasının 5. maddesi uyarınca, NATO üyesi bir ülkeye gerçekleştirilen saldırıya karşı bütün üye ülkelerin cevap verme hakkı bulunmaktadır." Bkz. a.e.

540 "Bir bireyin ağ üzerinde bulunan herhangi bir verisinin, verilerin gizliliği kapsamına girip girmediği hukuk uzmanları arasında halen bir inceleme ve tartışma konusudur. AB'nin Veri Koruma Yönergesi'ne göre tanımlanmış ya da tanımlanmamış gerçek kişilerin bilgileri kişisel veri olarak kabul edilir. Bu bakımdan bir kişinin ağ üzerindeki IP adresi yasa dışı yollardan elde edilirse hukuki olarak delil kabul edilemez. Yine aynı yönergeye göre bir kişi üçüncü bir ülkeye kişisel verilerini transfer ettiğinde ilgili ülkenin bu verileri koruma zorunluluğu vardır. Bu durumun suiistimal

kuralı”[541] , “erken uyarı kuralı”[542], “bilgileri kuralı”[543] , “suçluluk kuralı”[544], “manda kuralı”[545]. NATO, siber saldırılara karşı kendisini güçlendirmesi gerektiğini ilk kez 2002 Prag Zirvesi’ nde gündeme getirmiş, bundan sonra önemli gündem maddesine gelen siber saldırılara karşı 2008’ de ilk kez ortak siber savunma politikasını kabul etmiş, 2014’ te ise siber savunmayı ortak savunmanın bir parçası olarak kabul ederek 5. m.’ nin siber saldırı karşısında işletilebileceğine karar vermiş, siber tehditlerin giderek artması ve önem kazanmasıyla 2016 Zirvesi’ nde “siber alan” ı kara, hava ve denizin yanı sıra yeni harekat alanı olarak belirlemiş ve müttefiklerini sadece fiziki dünyada değil aynı zamanda siber ortamda oluşabilecek sınamalara karşı da korumayı taahhüt etmiş, 2018 Brüksel Zirvesi’nde ise yeni “Siber Operasyon Merkezi” kurma kararı almıştır.[546]

---

edilmesi ihtimaline karşılık yasal mevzuatla ilgili olarak uluslar arası bir düzenlemeye ihtiyaç duyulmaktadır.” Bkz. a.e.

541 “AB’nin Veri Koruma Yönergesi’ne göre, kişiler ağ üzerinden ya da yasal olmayan yollarla erişime karşı verilerin yanlışlıkla veya kasıtlı olarak yok edilmesini, değiştirilmesini, yetkisiz kişilere açıklanmasını önlemek amacıyla her türlü teknik ve organizasyonel önlemi almakla sorumludur. Aynı şekilde Avrupa Konseyi Sözleşmesi’nde (1981) kişilerin verilerini her türlü veri kaybı, yetkisiz kişilerin erişimi ve verilerin üçüncü kişilere açıklanması ile değiştirilmesini önlemek amacıyla gerekli önlemleri alması zorunluluğu hükmü 7. maddede açıkça belirtilmiştir. Bu kapsamda siber saldırıların siyasi boyutları arttıkça toplumsal, askeri ve bilgi hizmetleri açısından verilerin bakım ve korunmasına dair standartların geliştirilmesi gerekecektir.” Bkz. a.e.

542 “Servis sağlayıcılar, e-Gizlilik Yönergesi EC/2002/58’e göre hizmetlerinin güvenliğini korumak için her türlü teknik ve organizasyonel önlemleri almakla yükümlüdür. Gerektiğinde kamu iletişim ağı sağlayıcısı ile benzer eylemleri koordine etmek yükümlülü-güne sahiptir. Ayrıca e-Ticaret Yönergesine göre servis sağlayıcılar yasadışı faaliyetleri üye devletlerin yetkililerine derhal bildirmek zorundadırlar.” Bkz. a.e., s. 160.

543 “Halkın yaşam, güvenlik ve refahına yönelik tehditler hakkında bilgi sahibi olma hakkı vardır. Avrupa’da toplumların kamusal yaşam ve refahlarına yönelik tehditleri ve bu tehditler karşısında alınan kararları öğrenmek konusunda devletlerin şeffaf olması gerektiğine dair bir yargı gün geçtikçe daha güçlü olarak varlığını hissettirmektedir. Tehditlerin ve bu durumlar karşısında alınan kararların erişime açık olması kamuoyunun bilgilen-dirilmesi ve siber güvenlik açısından bilinçlendirilmesini sağlarken istenmeyen bilgi ifşasına da neden olabilir. Buna rağmen yapılan saldırılar ve alınan tedbirlerin açıklaması yasal çerçevede stratejik iletişim ve kamu bilincinin arttırıl-ması bağlamında gereklidir.” Bkz. a.e.

544 “Her ulusun kendi ceza hukukuna en yaygın siber suçları dâhil etme sorumluluğu vardır. Uluslar arası ceza kanuna göre bir durumun sonucu ulusal ya da uluslar arası yasalara göre bir suç sayılmadığı sürece siber saldırı yapan kişiye yönelik bir yaptırım uygulanması mümkün değildir. Bu durumlardaki anlaşmazlıkların giderilmesi ve bir uyum oluşturulması için esas alınabilecek olan Avrupa Birliği Siber Suçlar Sözleşmesi’ne göre bir bilgi-sayar sisteminin tamamına ya da herhangi bir parçasına haksız erişimler yasal yükümlülükler çerçevesinde değerlendirilmelidir.” Bkz. a.e.

545 “Manda yönetimi siber güvenlik konusunda uluslar arası çabaların desteklenmesi ve koordinesini kapsamaktadır. Siber güvenlikle ilgili olarak yasal ve politik araçlar açısından uluslar arası koordinasyonu ve boşlukları ortaya koymayı hedeflemektedir. Bugün bu uyum sağlama çabası hali hazırda hala en az 6 uluslar arası örgütün çalışma planında yer almaktadır. NATO, üye ülkelere gerçekleştirilen siber saldırılara karşı hangi durumlarda silahlı saldırı gerçekleştirilebileceği konusunda net bir karara varamamıştır. Bu bağlamda ülkelerin ortaklaşa ve koordineli olarak çalışmaları ve strateji geliştirmeleri gerekliliği ortadadır .” bkz. a.e.

546 “ **“NATO Siber Hızlı Tepki” timi 24 saat göreve hazır**

“İttifakın genel caydırıcılık ve savunmasını güçlendirmek için havada, karada ve denizde olduğu gibi siber alanda da etkili şekilde faaliyet gösterebilmeliyiz.” ilkesiyle hareket eden NATO, siber alanda uluslararası hukukun geçerli olduğunu savunuyor.

Siber güvenlik raporuna göre dünya ekonomisine verdiği toplam zararın 2015 yılında 3 trilyon dolar, 2021 yılında ise yaklaşık 6 trilyon dolar olacağı tahmin edilen[547] siber saldırılarla mücadele edebilmek içinse uluslararası şirketler, finans kuruluşları ve hükümetlerin adeta seferberlik ilan ettiği, İngiltere' nin 2016 yılında beş yıllık Ulusal Siber Güvenlik Stratejisini açıkladığı, 2017 yılında hükümete bağlı iletişim ve istihbarat kurumu "GCHQ"[548] nu altında özellikle ulusal boyutta veri güvenliğini tehdit edebilecek siber saldırıları belirlemek ve engellemek için çalışan Ulusal Siber Güvenlik Merkezi' ni kurduğu, ABD tarafında ise 2019 yılının nisan ayında Stratejik Kuvvetler Komutanlığı' na bağlı bir alt komutanlık olan "Siber Güvenlik Komutanlığı" nı bağımsız bir komutanlığına yükseltildiği, 2018 Ulusal Savunma Strateji Belgesinde savaş alanı olarak tanımladığı ve böylelikle siber güvenlikte fiili adımın atıldığı, 2019 yılının eylül ayında ise ABD' nin kritik altyapı ve kurumlarının veri tabanlarının siber saldırılara karşı güvenliğinin sağlanmasına vurgu yapılan ve ülkede siber suç işleyenlere yönelik ihbar ve yasal işlem yapma konusunda daha etkili sistemlerin kurulmasını içeren düzenlemelerin yer aldığı Ulusal Siber Güvenlik Strateji Belgesi' nin imzalandığının duyurulduğu, Rusya' nın, yerli yapım mobil işletim sistemine kademeli geçiş için 160 milyarlık bütçe ayırdığı ve sürecin 2021 yılında tamamlanacağı, Rusya' nın küresel internetle bağlantısının bir süreliğine

---

Siber savunma alanında eğitim ve tabikatlara çok önem veren NATO'ya bu çerçevede, Estonya'nın başkenti Tallinn'de bulunan ve ittifaka akreditasyonu olan Siber Savunma Mükemmeliyet Merkezi katkı sağlıyor.
NATO müttefikleri, ortak siber savunma kapasitelerini geliştirmek, siber saldırıları engellemek ve bu saldırıların etkilerini azaltmak için bilgi paylaşımında bulunuyor. İttifaka, misyon ve operasyonları için ülkelerin ulusal siber savunma kapasitelerini kullanma hakkı da sağlanıyor.
Diğer yandan ittifak, müttefiklere 24 saat yardım sağlayabilmek için "NATO Siber Hızlı Tepki" timini hazırda tutuyor.
Siber savunma alanında daha etkili olmak için NATO, hem konuyla alakalı işletmelerle hem de Avrupa Birliği (AB) ile işbirliği geliştiriyor. Öyle ki birlikte eğitim ve tatbikatlar yürüten, bilgi paylaşımında bulunan NATO ve AB için siber, temel iş birliği alanlarından birini oluşturuyor.
Siber saldırıların giderek daha karmaşık hal almaya başladığı ve gerek devlet gerekse devlet dışı aktörlerce sıklıkla kullanılmaya başladığı dönemde, siber alanının NATO için önemini artarak korumaya devam etmesi bekleniyor." Bkz. BASIN İLAN KURUMU, "Nato siber savunmaya odaklanıyor", Editör: Mevlüt Çiftçi, 30.08.2019, https://www.bik.gov.tr/nato-siber-savunmaya-odaklaniyor/, ET. 15 Şubat 2020.

547 Refik Samet ve Ömer Aslan, "Kötü Amaçlı Yazılımlar ve Analizi", *Siber Güvenlik ve Savunma : Farkındalık ve Caydırıcılık*, Ed.: Şeref Sağıroğlu, Mustafa Alkan, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, 1. bs., Grafiker Yayınları, Ankara, 2018, ss. 227-251, s. 226.

548 "GCHQ (İngilizce: Government Communications Headquarters), İngiliz devletini siber saldırılara ve tehditlere karşı korumak amacıyla hükûmet tarafından görevlendirilen güvenlik ve istihbarat kurumu. Devlet Başkanına veya ilgili kurum için bu tür saldırılara karşı nasıl hareket edileceğine dair bilgi ve danışmanlık sağlar. Kurum ilk başlarda 1919'da ve İkinci Dünya Savaşı sırasında Bletchley Parkı merkez üssü seçip, telekomünikasyon sistemlerinin çok büyük bir önem arz ettiği bir zamanda bu sistemlerin şifrelerini kırmayı başarmıştır. Bugün ise kurum siber güvenlik hizmetlerine ek olarak kimyasal, biyolojik ve nükleer silahlara ve tehditlere karşı önlem almak ve durdurmakla yükümlüdür…" bkz. https://tr.m.wikipedia.org/wiki/GCHQ, ET. 20 Şubat 2020.

kesilmesinin planlandığı böylelikle ülkede interneti küresel internet sağlayıcılardan bağımsız bir şekilde çalışacak hale getirerek olası siber saldırılardan korunmayı planladıkları, internetin yerelleştirilmesi için 20 milyar rublelik bütçe ayrıldığı, 1981 tarihli Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesini 2005' te onayladığı, Federal Kişisel Veriler Yasası' nı ise 2006' da kabul ettiği ancak 2014' te ise Kişisel Veri Yerelleştirme Yasası' nın 2014' te yürürlüğe girdiği böylelikle vatandaşlara verilerini yerel veri tabanlarında tutmayan web sitelerini engelleme seçeneğinin de sunulduğu, Avrupa Birliği' nde ise, AB Konseyi, Avrupa Parlamentosu ve AB Komisyonu arasında yapılan müzakereler sonucunda 2018 yılı aralık ayında yeni "Siber Güvenlik Yasası" üzerinde uzlaşı sağlandığı, kabul edilen yasa ile Avrupa Ağ ve Bilgi Güvenliği Ajansı' na ("ENISA"[549]) üye ülkelere siber güvenlik tehditleri ve saldırılarına karşı daha iyi destek sağlamak için kalıcı biçimde AB Siber Güvenlik Ajansı görevi verilmesinin öngörüldüğü, bunun yanında dijital hizmetlerin ve cihazlarının siber güvenliğini artırarak güvenlik sertifikaları için AB çerçevesi oluşturmayı amaçladığı belirtilmektedir.[550]

Türkiye' nin ise en fazla siber saldırıya uğrayan ülkeler arasında olduğu, siber saldırı sıralamasında sekizinci sırada, spam sıralamasında beşinci sırada, saldırı kökenli sıralamada ise on ikinci sırada yer aldığı, Türkiye' deki bilgisayarların % 45' inin saldırıya uğradığı, web uygulamaları ataklarında beşinci sırada, Avrupa' da ise dördüncü ülke olduğu belirtilmektedir.[551] Ülkemizde ise Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde oluşturulmuş olan Ulusal Siber Olaylara Müdahale Merkezi (USOM) 7 gün 24 saat esasına göre kritik altyapıları anlık izleyerek saldırıları önlemek ve bertaraf etmek için çalışmakta olup USOM koordinesinde bugüne kadar

549 ENISA' nın siber güvenlik raporları için bkz. https://afyonluoglu.org/siberguvenlik/nist-reports/, ET. 3 Mart 2020.

550 BASIN İLAN KURUMU, "Dünya 6 trilyon dolarlık siber saldırı riskine karşı hazırlanıyor", Editör: Mavlüt Çiftçi, 15.03.2019, https://www.bik.gov.tr/dunya-6trilyon-dolarlik-siber-saldiri-riskine-karsi-hazirlaniyor/, ET. 18 Şubat 2020.

551 "Ünlü bir otomobil üreticilerinden birisinin en son model araçlarından bir tanesi White Dergisi editörleri tarafından bilinçli bir şekilde hacklendi ve araba kendi kendine yürüdü. Bir mobil telefonla aracı kumanda etmeye başlayan editörler, aracı çalmak niyetinde değildi. Sadece nesnelerin interneti sisteminde ne kadar güvensiz ve korumasız olabileceğini göstermek istiyorlardı. Bugünkü hukuk yapısı, bu sorunların büyük bir çoğunluğuna şu anda yanıt veremiyor…" bkz. Faruk Eczacıbaşı, "Siber Risklerin Yönetimi", "1. Oturum Dünya ve Türkiye'deki Siber Tehditler ve Hayatımıza Etkileri", *Risk Management Forum 2015*, Nart Sigorta ve Reasürans Brokerliği A.Ş., 1. Bsk., İstanbul, 2016, ss. 25-27, s. 26.

sonuncusu 20 Aralık 2019' da gerçekleştirilen "Siber Kalkan"[552] siber güvenlik tatbikatı olmak üzere toplamda 5 adet siber güvenlik tatbikatı gerçekleştirilmiştir.

1.2.5.3.2. Siber Saldırı Türleri ve Kullanılan Kötü Amaçlı Yazılım Çeşitleri

Önceleri basit ve belli bir amaç doğrultusunda gerçekleştirilmeyen siber saldırılar, yerini daha geniş çaplı ve hedef odaklı saldırılara bırakmış olup yapılan araştırmalar siber saldırıların büyük bölümünün kullanıcı bilgisi dışında sistem üzerinde istenmeyen değişiklikler yapan yazılımlar olarak tanımlanabilen kötü amaçlı yazılımlar (Malicious Software - Malware) (Truva atları, virüsler, solucanlar, yazılım bombaları, fidye yazılımları, robotlar ve casus yazılımlar gibi) kullanılarak yapıldığını göstermiştir.[553] Çoğunlukla sistemlerin güvenlik açıklarını kullanarak gerçekleştirilen siber saldırılara karşı yazılım şirketleri sürekli güncellemelerle önlem almakta iseler de esasen öngörülemeyen açıkların var olabileceği de yadsınamaz bir gerçektir. Nitekim, IOS 12 sürümünde bir saldırganın herhangi bir etkileşim olmadan IOS cihazı üzerindeki dosyaları uzaktan yetkisiz bir şekilde okunmasını sağlayabilecek bir güvenlik açığı tespit ederek IOS 12.4 güncellemesinin gerçekleştirilmesi, Linux çekirdeğinde hak ve yetki yükselten kritik bir güvenlik açığının tespit edilerek Linux kernel sürümünün son versiyonuna güncelleştirilmesi bunlara birer örnek oluşturmaktadır.[554] Biz de bu başlık altında gerçekleşecek siber saldırılar neticesinde hangi sistemlerin etkilendiği, hangi verilerin zarar gördüğü, değiştirildiği veya çalındığını önceden belirleyebilmek adına konuya ışık tutması bakımından saldırı türlerini bir diğer deyişle bilişim suçlarının işlenme yöntemlerine değineceğiz.[555] Siber saldırganların kişilerin ve her ölçekteki organizasyonun bilişim teknolojilerinin sunduğu imkânları ve bilişim sistemlerinin açıklarını kullanma yönünde her gün neredeyse bir yenisi eklenen yöntemler kullanarak bankamatik şifresini kopyalamak gibi basit bir eylemden başlayıp toplumdaki güven duygusunu zedelemeye, terörist eylemlere, hedef ülkenin bilişim sistemlerine çeşitli gruplar vasıtasıyla saldırmaya varıncaya kadar değişik hedeflere karşı saldırılar gerçekleştirebildiklerinden, bilişim

552 Bkz. BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, "Siber Kalkan 2019 Sona Erdi", 20 Aralık 2019, www.btk.gov.tr/haberler/siber-kalkan-2019-sona-erdi, ET. 18 Şubat 2020;
International Telecomunication Union, "Cyber Shield 2019" https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/CyberShield/Cyber-Shield-2019.aspx, ET. 24 Şubat 2020.
553 Samet ve Aslan, a.g.e., s. 225, 226.
554 CYBERMAG, "Privia Security Ağustos Ayı Siber Güvenlik Gelişmeleri Bülteni", Sayı: 44, Eylül 2019, ss. 30-33, s. 32.
555 Samet ve Aslan, a.g.e., s. 225, 226.

dünyasının hızlı gelişimine paralel olarak her geçen gün ortaya çıkan yeni saldırı türlerinin hıza yetişmek mümkün bulunmadığından bu başlık altında incelenecek olanlar bazı örneklerden ibaret olup belirtmek gerekir ki saldırgan veya bilişim suçu faillerinin yeni veya farklı yöntemleri kullanması mümkün olacaktır.[556]

Saldırılar genelde elektronik e-posta ve internet tarayıcılarındaki savunmasızlıklardan yararlanarak tüm dünyayı etkileyen ve çok sayıda bilgisayar kullanılarak gerçekleştirilen (örneğin, BOTNET) küresel tehditler, belli kurum ve kuruşlara yönelik yapılan, hedefinde genelde kurumların finansal kaynakları ve popülerliklerine zarar verme fikri yatan ve hedef odaklı olan gelişmiş kalıcı/sürekli tehditler ("APT"[557]- Advanced persistent threat) ve saldırı yapılan sisteme aşırı miktarda büyük boyutlu veriler göndererek ya da çok farklı kaynaktan sürekli benzer veriler göndermek suretiyle sistemin cevap veremez hale getirilmesi şeklinde gerçekleştirilen ve genelde savunmasız bilgisayarlar (Zombi) kullanılarak yapılan ve "TCP/IP protokol yapısındaki açıklardan faydalanarak veya bir sunucuya çok sayıda istek yönelterek sunucunun iş göremez hale gelmesini sağlayan"[558] "hizmeti engelleme saldırıları"[559] ("DOS"[560]) şeklinde sınıflandırılabilmekte olup ileri düzey

556 Fazıl Gürler, *Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar*, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Yüksek Lisans Tezi, Ankara, 2013, s. 60, 61, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

557 "Gelişmiş Sürekli Tehdit (GST), bir kişi veya grubun bir ağa yetkisiz erişim sağladığı ve uzun bir süre boyunca algılanamadığı bilgisayar ağı saldırısıdır. Bu tür saldırılar genel olarak ticari veya politik amaç güden devlet sponsorluğu ile yapılan saldırılar olmasına rağmen, son birkaç yıl içerisinde devlet sponsorlığında olmayan belirli hedeflere yönelik geniş çaplı GST saldırıları da yaşanmıştır…" bkz. https://tr.m.wikipedia.org/wiki/Gelişmiş_Sürekli_Tehdit, ET. 20 Şubat 2020.

558 Ahmet Ünal, Bilişim Suç Türlerinden Biri Olan Dağıtık Servis Dışı Bırakma (DDoS) Saldırılarının Önlenmesindeki Hukuki ve Teknik Zorluklar, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, 2014, s. 13, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.
"Servis dışı bırakma saldırılarında hedef spesifik bir bilgisayar olabileceği gibi bir port ya da hedef sistemdeki bir servis, bir ağın tamamı, her hangi bir sistem bileşeni ve ya herhangi bir ağ bileşeni olabilir. Servis dışı bırakma saldırılarında hedef insan ve sistem iletişimi ya da insan cevap sistemleri arasında olabilir." Bkz. A.e., s. 14.

559 "... İnternet trafiğinin önemli bir bölümünün e-postalardan, posta trafiğinin yüzde yetmişinin de gereksiz postalardan oluştuğu düşünüldüğünde, gereksiz postaların önemi daha iyi anlaşılabilecektir. Bu nedenle gereksiz postalara, hizmet aksatma saldırıları içinde yer vermek daha doğru olacaktır. Gereksiz postaların özel yasalarla düzenlendiği ülkeler bulunmakta, ülkemizde ise genel veya özel olarak herhangi bir düzenlemeye gidilmediği görülmektedir." bkz. Karagöz, a.g.e., s. 81.

560 "Denial of Service (DoS saldırısı), internete bağlı bir hostun hizmetlerini geçici veya süresiz olarak aksatarak, bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından ulaşılamamasını hedefleyen bir siber saldırıdır. DoS genellikle hedef makine veya kaynağın, gereksiz talepler ile aşırı yüklenmesi ve bazı ya da bütün meşru taleplere doluluktan kaynaklı engel olunması şeklinde gerçekleştirilir. DoS saldırısını; bir grup insanın, bir dükkân veya işyerindeki kapıları tıkayıp, meşru tarafların mağazaya veya işletmeye girmesine izin vermeyerek normal işlemleri aksatması şeklinde örnekleyebiliriz DoS saldırılarının failleri genellikle bankalar veya kredi kartı ödeme sistemleri gibi yüksek profilli web sunucularında barındırılan siteleri veya hizmetleri hedef alır. İntikam, şantaj ve

tehditler olarak bilinen küresel tehditler, APT ve DOS saldırıları genelde birden fazla kötü amaçlı yazılım türü (örneğin, virüs, Truva atı, arka kapı, vb.) kullanılarak gerçekleştirilmekte ve birçok siber saldırının kökeninde kötü amaçlı yazılımlar bulunmaktadır.[561]

Bilişim sistemine veya hedefe sızmak için güvenlik sistemlerinin en zayıf halkası olarak görülen kullanıcıları yönlendirerek gerçekleştirilen[562], kişinin içerisinde bulunduğu zaafları kullanarak istenilen veriyi elde etmek veya karşı tarafı ikna veya başka bir yolla yanıltıp güvenlik süreçlerini atlatma hali olarak da ifade edilebilen "sosyal mühendislik"[563] saldırıları ise dört aşamalı olup ilk aşama kişinin karşı taraf

aktivizm bu saldırıları motive edebilir." Bkz. https://tr.m.wikipedia.org/wiki/Denial-of-service_attack, ET. 20 Şubat 2010.

561 Samet ve Aslan, a.g.e., s. 226.

562 Alper Başaran, *Siber Savaş Cephesinden Notlar*, Arıon Yayınevi, İstanbul, 2016, s. 33.

563 Europol' un 2011 yılı IOCTA Raporu, AB vatandaşlarının giderek artan bir şekilde siber suç etkinliği için bir hedef olan sosyal medya araçlarını kullanarak kişisel kimliklerini, gizliliklerini ve bilgisayar verilerini nasıl riske attığını incelemiştir:

"Son yıllarda dünya çapında web'in bir web sitesi koleksiyonundan sosyal ağ siteleri ve gerçek zamanlı iletişim araçları ('Web 2.0') gibi bağlantılı hizmetler için bir platforma geçiş, sosyal mühendisliğin genişletilmesi için teknik araçlar sağlamıştır. .

FaceBook gibi sosyal ağ sitelerinin kullanıcıları, profil sayfalarına kolayca fotoğraf veya video paylaşım sitelerinden içerik yerleştirebilir ve arkadaşlarıyla etkileşim kurmak için kullandıkları küçük uygulamaları, araçları ve oyunları yükleyebilir. Bununla birlikte, siber suçlular, kendilerini tanıdıkları "güvenli" bir ağda olduğunu düşünen kullanıcıların - yayınlanan öğelere kötü amaçlı yazılım enjekte ederek ve sahte ve kişisel bilgileri çıkarmak için tasarlanmış web sitelerinin bağlantılarını paylaşarak kullanıcıların güvenini kullanır.

Kuruluşların çoğu işyerinde sosyal paylaşım sitelerinin kullanımını kabul etmeye başlamıştır. Ancak doğru koşullar altında, işyerinde sosyal medyaya erişim, şirket ağlarına casus yazılımlarla bulaşma potansiyeline ve büyük miktarlarda kişisel, kurumsal ve finansal verileri kar elde etme potansiyeline sahiptir. ABD'deki küçük ve orta ölçekli işletmelerin% 33'ü sosyal ağ siteleri aracılığıyla dağıtılan kötü amaçlı yazılımlara bulaştığını söylüyor. Enfekte olanların% 35'i mali zarar gördü ve bunların üçte birinden fazlası enfeksiyon sonucu 5000 dolardan fazla kaybetti (kaynak: PandaLabs). Kuruluşlar, çalışanların izlemesi gereken sosyal medya yönergelerini belirleyerek bu riskleri azaltabilir.

Sosyal mühendislik - insanları eylemler gerçekleştirme veya gizli bilgileri ifşa etme eylemi - hacker kültürü ve siber suçlama yöntemlerinin temel bir özelliğidir. Kimlik avı ile ilgili suçlular, örneğin, e-posta alıcılarını, müşterilerin kişisel verilerinin doğrulanmasını gerektiren kuruluşları temsil ettikleri konusunda ikna etmeyi amaçlarken, sahte web siteleri, müşterilerini hesap ayrıntılarını açığa çıkarmak için tasarlanmış yasal çevrimiçi hizmetlerin sahte sürümleridir. İnternet kullanıcıları, işe yaramaz veya en kötü senaryo, suçlu yazılım ve güvenlik riskleri içeren anti-virüs yazılımı için ödeme yapmak için bile manipüle edilebilir.

'Gelişmiş ücret sahtekarlığı', düşük maliyet ve insanlarla iletişim kurma kolaylığı nedeniyle, internet çağında toptan dönüşüm geçiren sosyal mühendisliğin bir başka örneğidir. Gelişmiş ücret dolandırıcıları kurbanları ödül vaadiyle ikna eder ve bu suçla internet kullanıcıları var olmayan miraslar ve piyango kazançları için 'tahliye ücretleri' ödemeye devam ederler. Devam eden ekonomik krizin etkileri insanları dolandırıcılığa karşı daha duyarlı hale getirebilir. Bu nedenle internet kullanıcıları arasında farkındalığı artırmak, siber suçları başarılı bir şekilde önlemek ve mücadele etmek için çok önemlidir.

Kullanıcıların arkadaşlarını daha kolay çevrimdışı bulmasına ve sosyal ağ profillerine ('coğrafi etiketleme') bilgi eklemesine olanak tanıyan, kullanıcının nerede olduğunu ancak daha da önemlisi mevcut konumlarını bildiren çevrimiçi konum tabanlı hizmetler de geliştirilmiştir. İstatistikler, gençlerin% 69'unun fiziksel konumlarını sosyal ağ sitelerindeki güncellemelere dahil ettiğini gösteriyor (kaynak: McAfee). Endişeler, internet kullanıcılarının çevrimdışı konumlarını ifşa

hakkında bilgiler toplaması, ikinci aşama saldırganın toplamış olduğu bilgiler doğrultusunda karşı taraf ile iletişime geçmesi, bu bilgileri kullanması ve de amacı doğrultusunda kullanabileceği araçları tespit etmesi, üçüncü aşama artık uygulamaya geçerek ulaşmak istediği bilgilere ulaşması ve son aşama ise artık bu bilgileri istismar ederek istenilen nihai amaca ulaşması olarak ifade edilebilmektedir.[564]

Yine bilişim ağına fiziksel yolla girme ya da ilişim ağındaki elektromanyetik dalgaların hassas alıcılarla algılanması esasına dayanan "gizlice dinleme" adı verilen bir başka saldırı türü ise, bilgisayar sistemlerinde veri naklinde kullanılan ağlara fiziksel yolla (telefon hatlarındaki gibi) girilerek veya bilgisayarın az da olsa yaydığı elektromanyetik dalgaların sistemin yakınlarına yerleştirilecek hassas elektromanyetik dalga alıcıları vasıtasıyla yakalanıp verilerin elde edilmesi tekniğidir.[565] Askeri terimle TEMPEST denilen elektromanyetik yayın kaçağı ise TEMPEST koruması olmayan elektronik cihazlardan ve özellikle CRT türü ekranlardan birkaç yüz metreye kadar uzaktan özel anten ve cihazlarla bilgi alınabilmekte olup TEMPEST önlemleri halen askeri ve diğer bazı devlet uygulamalarında önemli görülmekte ancak sivil uygulamalarda henüz yaygınlaşmamıştır.[566] Hukuka aykırı ırkçı, ayrımcı, bölücü, terörü ve şiddeti teşvik eden, kişilik haklarına aykırı, insan ticareti veya çocuk pornografisi vb. içeriklerin, web sayfaları, forumlar, elektronik postalar ve dosya paylaşımı gibi veri iletim ağları aracılığı ile diğer kullanıcıların erişimine sunulması olarak tanımlanabilecek "hukuka aykırı içerik sunma" da bir başka saldırı yöntemidir.[567] "Sistemi kırıp içeri girilmesi" (hacking) ise hedef bilişim sistemine girmek isteyen kişiler amaçlarına sistemlerin (açık kapılarını bularak) şifrelerini kırıp, koruma duvarlarını (firewall) aşmak yoluyla ulaşılmakta olup genellikle sisteme giriş sırasında yardımcı yazılımlar kullanılmamakta ve fiilin bilişim korsanı (hacker) veya korsanları tarafından gerçekleştirilmektedir.[568]

---

etmeye istekli oldukları konusunda dile getirilmektedir, çünkü kişisel mülklerini gözetimsiz bıraktıklarını açıkça belirtenlerin açık bir güvenlik riski vardır." Bkz. EUROPOL, "THE HIDDEN RISKS OF SOCIAL MEDIA", Europol, 5.01.2011, https://www.europol.europa.eu/newsroom/news/hidden-risks-of-social-media, ET. 1 Mart 2020. (Google Translate ile çeviri yapılmıştır.)

564 Barış Emre Alp, *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu*, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara, 2018, s. 30,31, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

565 Gürler, a.g.e., s. 69.

566 İnce, a.g.e., s. 164.

567 Gürler, a.g.e., s. 70.

568 "Önceleri bilişim sistemlerine iyi niyetle girerek sistemin açıklarını bularak düzeltilmesini isteyen kişilere "hacker" adı verilirken, sisteme girme işlemine "hacking" denilmekteydi. Ayrıca ilk

Sistemde mevcut açıkları kullanarak verileri elde etme, değiştirme ya da yok etme gibi amaçlarla kullanılan kötü amaçlı yazılımlar hükümetler, işletmeler ve son kullanıcılar için en tehlikeli siber saldırı araçlarından sayılmakta olup bu uygulamalar yazılımsal olabileceği gibi cihazın içine yerleştirilen küçük bir aygıt ile klavyeden girilen her türlü bilgiyi kaydedebilen klavye dinleme cihazları gibi donanımsal da olabilirler.[569] Bununla birlikte saldırılar mutlaka ağ üzerinden yapılmak zorunda olmayıp kötü amaçlı yazılımlar ağ bağlantısı olmayan cihazlara yüklenerek de veri hırsızlığı gerçekleştirilebilmektedir.[570] Örneğin, ATM ve POS cihazlarına yüklenen casus yazılımlar sayesinde kullanıcının verileri yasadışı olarak ele geçirilebilmektedir.[571]

Aşağıda başlıklar halinde sıralanmış olan kötü amaçlı yazılım türleri ile gerçekleştirilen siber saldırı türleri de sınırlı sayıda olmayıp uygulamada da sıklıkla karşılaşılan saldırı türlerini oluşturması açısından örnekleme yolu ile incelenecektir.

1.2.5.3.2.1. Virüsler

Çoğalmaları için başka programlara ihtiyaç duyan ve içinde kötü amaçlı kod parçacıkları barındıran programlar olan virüsler, diğer programlara kendilerini enjekte ederek bu programların da virüs haline gelmelerine neden olmakta, girdiği sistemlerde sistem dosyalarında değişiklik yaparak çalışmaz hale getirebilmekte, istenmeyen görüntülerin ekranda görünmesine neden olabilmekte ya da veriler üzerinde değişiklik yapabilmektedirler.[572] Virüsler, esasen solucanlar ve Truva atı gibi kötücül yazılımların bir üst yapısını oluşturmakta olup solucanlardan dosya ve yazılımlar aracılığıyla yayılabilmeleri, sisteme zarar vererek dolaşmaları yönlerinden; Truva Atı'ndan ise, sisteme izinsiz girmeleri yönünden ayrılmaktadırlar.[573] Örnek vermek

başlarda kötü niyetli olarak bilişim sistemine girme veya zarar vermeye "crack" eylemi ve eylemi yapanlara ise "cracker" adı veriliyordu. Ancak zamanla bu detayı bilmeyen kamuoyunda crack ve hacking eylemi ile cracker ve hacker kavramları özdeşleşti. Sisteme girme niyetine bakılmaksızın (kötü niyetle girme anlamında) hacking ve hacker kavramları kullanılmaya başlandı.300 Hacker teriminin karşılığı olarak Türkçede "bilişim korsanı" terimi kullanılmaya başlandı." Bkz. A.e., s. 80. "Hacking günümüzde bilgisayar sistemlerine yetkisiz erişim sağlanması eylemine karşılık olarak kullanılmakta iken hacker terimi ise eylemi gerçekleştiren kişiye verilen addır. Hacking eylemi, internet üzerinden gerçekleştirilen bir tür ihlaldir. Bilgisayar ağlarında bulunan güvenlik açıklarının tespit edilerek bilgisayara ya da ağ sistemine yetkisiz erişim sağlanmasıdır." Bkz. Eryaman, a.g.e., s. 15.

569 Yılmaz ve Sağıroğlu, a.g.e., s. 162, 163.

570 A.e.

571 A.e.

572 Samet ve Aslan, a.g.e., s. 229.

573 Gürler, a.g.e., s. 65.

gerekir ise “Creeper”, “Chernobly (CIH)” “Melissa” ve “ILOVEYOU” ise yaygın olarak bilinen virüslerdir.[574]

1.2.5.3.2.2. Truva Atları (Trojans)

Yunan efsanesinden gelen, kendi orijinal adını değiştirebilen ve bilgisayarın her açılışında yeniden aktif hale geçebilen truva atları, yararlı bir program kisvesi altında kötü niyetli yazılımlar aracılığıyla sızmayı ifade etmekte olup özellikle bilgisayarın işletim sistemi içerisinde kendisini saklamakta, üremeye ve yayılmaya yönelik otomatik mekanizmalar bulundurmasa da elektronik postaların veya web sayfalarının arkasına gizlenerek elektronik postaların veya web sayfalarının yüklenmesi durumunda aktif hale geçebilmektedirler.[575] Başka bir anlatımla, sistemleri etkileyebilmeleri için iliştirilen programın çalıştırılması gerekmekte olan bulaştığı sistemleri genelde yavaşlattıkları için varlıkları ancak uzun uğraşlar sonucunda öğrenilebilen ve virüsler ve solucanlar gibi başka dosyaları enfekte ederek çoğalmayan veya kendi kendini kopyalamayan bu tür yazılımlar sistemde arka kapılar açabilmekte, girdiği sisteme izinsiz olarak uzaktan erişime neden olabilmekte ya da bilgisayarda depolanan kritik bilgileri karşı tarafa gönderebilmektedir.[576] Örneğin Haziran 2019’ dan itibaren Türkiye’ de yoğun faaliyet gösteren Anubis adlı Truva atının, siber saldırganların önde gelen bir telekomünikasyon ve teknoloji hizmetleri sağlayıcısından ücretsiz internet bağlantısı teklifi gibi gönderdiği SMS’lerde SMS’ te yer alan bağlantıya tıklandığında indirildiği, bu Truva atının indirildikten sonra SMS gönderme, alma, silme, kişi listesini, hesap giriş bilgilerini çalma, URL açma, mobil cihazlarda saklı dosyaları şifreleme, ses kaydetme, ekran görüntüsü alma, tuş takibi yapma, kullanıcıların kimlik bilgilerini çalmak için sahte giriş sayfaları gösterme gibi faaliyetler gerçekleştirebildiği belirtilmektedir.[577] Bankaların bilişim sistemine girilerek hukuka aykırı yarar sağlanması, devletlerin veya bilimsel veya askeri kuruluşların bilişim sistemlerine sızma suretiyle milli güvenlik ve istihbarat bilgilerinin çalınması gibi casusluk fiilleri ise çoğunlukla Truva Atı saldırıları ile gerçekleştirilmektedir.[578]

574 Samet ve Aslan, a.g.e., s. 229.
575 Çakmak ve Demir, a.g.e., s. 73.
576 Samet ve Aslan, a.g.e., s. 230.
577 CYBERMAG, “Anubis Truva Atından Türkiye’ye Yoğun Saldırı”, Sayı: 44, Eylül 2019, ss. 40-41, s. 40.
578 Gürler, a.g.e., s. 74, 75.

Bankacılık Truva atları olarak da ifade edilen finansal zararlı yazılımlar ise siber suçlular ve dolandırıcıların en öncelikli motivasyon kaynağı olan para ve finansal verileri çalmak için kullanılan, kurumsal ağların genellikle bağlantılı cihazlardan oluşması sebebiyle de bir cihazın ele geçirilmesiyle tüm kurumu tehdit altında bırakabilen güncellenmemiş cihazlardaki açıkları kullanarak yayılan bir yazılım türüdür.[579]

1.2.5.3.2.3. Solucanlar

Bilgisayar ağlarını kullanarak bir sistemden diğerine bulaşan, bulaştığı sistemlerde genelde izinsiz girişlere neden olan programlar olan solucanlar, virüslerin aksine çoğalmaları için başka programlara ihtiyaç duymamakta olup bulaştığı sistemde kendilerini gizleyebilmek için kendi dosyalarını silmekte ve genelde sistemlerde arka kapı açarak bu sistemleri başka saldırılarda kullanmaktadırlar.[580] "Code Red", "Nimda", "MyDoom", "Conficker" ve "Stuxnet" ise yaygın olarak bilinen bilgisayar solucanlarına örnektir.[581]

1.2.5.3.2.4. Arka Kapılar

Diğer güvenlik mekanizmalarını aldatmak için sözde kapı açan ve uzaktan erişim imkanı veren bir uygulama veya hizmeti ifade eden arka kapılar genellikle işletim sistemi ya da paylaşım yahut bedava yazılımlar içerisinde bulunmakta olup ayrıca elektronik posta ya da diğer kötü amaçlı yazılımlar üzerinden de yayılabilmektedirler.[582]

1.2.5.3.2.5. Oltalama (Phishing)

Kullanıcıya bir işlem yapması gerektiğini anlatan, bu işlem için tıklanması gereken bir bağlantı ya da indirilmesi gereken bir ek içeren bir elektronik postanın gönderilmesi ile başlayan ve kullanıcıların kimlik bilgilerini veya bankacılık bilgilerini çalmayı amaçlayan saldırılardır.[583] Güvenilen bir kurumdan gelen e-postaya şifre

579 "Bu zararlı yazılımların en yaygın saldırı vektörlerini spam e-postalar ve kimlik avı web sayfaları oluşturuyor. Kimlik avı web sayfaları, gerçek ve yasal sayfalar gibi görünüyor fakat aslında tehdit grupları tarafından hazırlanıyorlar. Bu sayfalar kimlik ve banka kartı bilgilerini veya başka hassas bilgileri ele geçirmekte kullanılıyor." Bkz. A.e., s. 38.
580 Samet ve Aslan, a.g.e., s. 229.
581 A.e.
582 Çakmak ve Demir, a.g.e., s. 73.
583 Başaran, a.g.e., s. 30.

yazılırken esasen yazılan bilgilerin faile gönderilmesi işlemi gerçekleşmekte olup oltalama saldırılarının birkaç çeşidi bulunmakla beraber sıklıkla banka bilgilerini çalmak için sahte e-posta ekranları oluşturulmaktadır.[584] Siber saldırganlar farklı kimlikte biri gibi davranarak e-posta, telefon veya yazılı bir mesaj yolu ile karşı taraf ile irtibata geçip kişinin kişisel verilerini, banka hesabı veya kredi kartı bilgileri gibi hassas verilerini elde ederek daha sonra önemli başka hesaplara erişebilmek için bunları kullanabilir sonuç itibariyle kimlik hırsızlığı veya mali kayıplar gibi sonuçlar ortaya çıkabilmektedir.[585]

Oltalama saldırı yönteminde hedefte olan binlerce bilgisayar kullanıcısına, içeriği sanki gerçek sahibinden geliyormuş gibi görünen, müşteri bilgilerinin güncellenmesi, kullanıcı adı ve şifresinin süre aşımına uğradığı, şifrelerin değiştirilmesi gerektiği, yarışma olduğu, ödül veya hediye kazandığı kişisel bilgilerini vermesi gerektiği vb. konulu sahte ileti yem olarak gönderilmekte, *bu maile* cevap verenler ve/veya işlem yapanlar gerçek internet sitesini taklit eden sayfaya yönlendirilmekte ve yönlendirilen sayfalarda bulunan kullanıcıdan istenilen kişisel bilgilerin (şifreler, kullanıcı adları vs.) ve finansal hesap erişim bilgilerin (online bankacılık ve kredi kartı numaraları, güvenlik kodları) doldurulması ile de bu bilgiler saldırganların eline geçmektedir.[586] Türk Ceza Kanunu'nun 245. m.' sinde düzenlenen banka ve kredi kartlarının kötüye kullanma suçu işlenmesi mümkün hale gelmektedir.[587]

1.2.5.3.2.6. Casus Yazılımlar (Spyware)

Çeşitli amaçlarla kullanıcı bilgisini ve faaliyetlerini izleyen, toplayan ve bir kuruma veya şirkete ileten bu yazılımlar çoğunlukla arka planda ortaya çıktığından faaliyetleri çoğu kullanıcı için fark edilmemekte[588] web sitelerine ya da ücretsiz paylaşılan yazılımlara gömülerek yayılmaktadırlar ve bu siteler ziyaret edildiğinde veya bu programlar bilgisayarınıza indirildiğinde sisteminize bulaşmaktadırlar.[589]

584 Hüdaverdi Uçar, *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü*, Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı Yüksek Lisans Tezi, Ankara, 2014, s. 33, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.
585 CYBERMAG, "CISCO Orta Doğu ve Afrika Siber Güvenlik Direktörü Fady Younes İle Söyleşi", Sayı: 45, Ekim, 2019, s. 9, ss. 6-15.
586 Gürler, a.g.e., s. 77, 78.
587 Uçar, a.g.e., s. 33.
588 Çakmak ve Demir, a.g.e., s. 73.
589 Bu yazılımlara örnek olan "Keylogger", arka planda çalışıp klavyeden yapılan her vuruşu kaydeden ve bu kayıtları saldırganlara gönderen programlardır. Bkz. Samet ve Aslan, a.g.e., 231.

Casus yazılımlar bir virüs türü olmadığından anti-virüs programları ile silinmeleri mümkün bulunmayıp bu tür programların "Casus Yazılım Temizleme Programları" sayesinde bilgisayarlardan silinebilmeleri gerekir bunun yanında firewall' lar (Koruma Duvarı) kullanılmalı ve devamlı güncelleştirilme yapılması gerekmektedir.[590]

Temmuz 2019' da dünyanın en yaygın kullanılan mesajlaşma uygulaması olan WhatsApp üzerinden telefonlara casus yazılım yerleştirildiği, WhatsApp' ın yayımladığı çağrı ile 1,5 milyar kullanıcından uygulamayı güncellemesi istendiği belirtilmektedir.[591]

1.2.5.3.2.7. Fidye Yazılımları (Ransomware)

Bulaştığı sistemde sistemin bir kısmını veya tamamını şifreleyerek verilerin kullanıcı tarafından görüntülenmesini engelleyen programlar olan fidye yazılımları ile saldırgan, kullanıcının verilerini görüntüleyebilmesi için kullanıcıdan talep ettiği parayı ödemesini beklemekte, paranın ödenmesi ise sistem verilerine erişimi garanti etmemektedir.[592] Siber saldırganlar saldırıdan önce tüm yedekleri silerek saldırıda bulundukları kurumu veya şirketi çaresizliğe sürükleyerek fidye ödemeye zorlayabilmektedirler.[593] Genellikle e-posta üzerinden kullanıcının e-posta içeriğinde yer alan bir bağlantıya tıklanması ya da zararlı bir eklentiyi açması ile gerçekleşen fidye yazılımı ile yapılan saldırılarda kullanıcının verileri önceden belirlenen fidyeyi ödeyene kadar şifrelenmekte, ödeme yapıldığında saldırgan kurbanın şifrelenmiş verilerinin şifresini çözecek bir kod gönderilmektedir.[594] "Wannacry" (2017), "NotPetya" (2016), "SimpleLocker" (2015-2016), "CryptoLocker" (2013-2014), "WinLock" (2010) yaygın olarak bilinen fidye yazılımlarına örnektir.[595]

---

590 Gürler, a.g.e., s. 68.

591 "Elde edilen bilgiye göre, siber saldırganlar, WhatsApp'ın sesli arama özelliğini kullanarak, hedef kişinin telefonunu çaldırdı. Üstelik bu kişi aramaya yanıt vermemiş olsa bile, casus yazılım telefona yerleştirilebildi. Ayrıca, bu kötü niyetli arama, hedef kişinin cihazındaki son gelen aramalar listesinden de silindi." Bkz. CYBERMAG, "WhatsApp Üzerinden Telefonlara Casus Yazılım Yerleştirildi", Sayı: 42, Temmuz 2019, s. 35.

592 Samet ve Aslan, a.g.e., s. 230.

593 CYBERMAG, "Artık Milyonlarca Kişinin Değil, Milyonlarca Doların Peşine Düşüyorlar", Sayı: 36, Ocak 2019, ss. 30-31, s. 30.

594 Eryaman, a.g.e., s. 9.

595 Samet ve Aslan, a.g.e., s. 230.

"28 Ağustos'ta Cenevre'de düzenlenecek bir İTÜ çalıştayı, gelişen siber güvenlik ortamını ve siber saldırıların gelişmişlik kazanmasıyla hafifletilecek yeni tehditleri tartışacak. Atölye, özellikle kurbanların veri fidye tutmak için tasarlanmış kötü amaçlı yazılım artan yaygınlık yanıt verir.

Atölye saldırı senaryoları araştıracak - CryptoLocker ve WannaCry gibi durumlarda soruşturma - ve sanayi ve hükümet tarafından istihdam ilişkili korumalar, tehdit-istihbarat paylaşımı da dahil olmak üzere saldırıların bulaşmasını önlemek için.

1.2.5.3.2.8. Robot Yazılımlar (Bots)

Bir dizi robotlardan oluşan botnetler, zafiyetli bilgisayar ve sistemlere veriler göndererek daha sonra bu bilgisayarları yapacakları saldırılarda kullanılırlar, sistemleri çalışmaz hale getirebilirler, zombi olarak kullanılan bilgisayarlardan önemli bilgiler çalabilir ya da zombi bilgisayarları para karşılığı üçüncü kişilere kiraya verilebilirler.[596] Başka bir anlatımla, birbirleriyle internet üzerinden iletişim kuran bilgisayarlardan oluşan botnet, spam göndermek, dağıtılmış hizmet reddi (DDoS) saldırıları ve diğer suçları işlemek için kullanılmaktadır.[597]

1.2.5.3.2.9. Yeni Nesil Kötü Amaçlı Yazılımlar

Yukarıdaki başlıklar altında işlemiş olduğumuz ilk zamanlarda basit amaçlarla yazılan zararlı yazılımlar ve kötü amaçlı yazılımların atası olarak kabul edilen virüsler zamanla şekil ve yöntem değiştirerek geleneksel kötü amaçlı yazılımların oluşmasına ve daha da gelişerek zamanla yerini geniş çaplı büyük şirketlerin ve devletlerin olduğu, ileri düzey siber saldırıların başlatılabildiği yeni nesil kötü amaçlı yazılımlara bırakmıştır.[598] Örneğin güncel bir kötü amaçlı yazılım örneği olarak bilgi çalan Zegost zararlı yazılımı karmaşık yapıda teknikler kullanıp iyi gizlenerek uzun vadeli uzun vadeli olmayı amaçlıyor.[599] Bu yazılımların analizi, özellikleri teknik anlamda

---

Çalıştay bulguları, 29 Ağustos- 7 Eylül 2018 tarihleri arasında toplanan İTÜ'nün 'BİT kullanımında güven ve güvenlik oluşturmaktan' sorumlu standardizasyon uzman grubu İTÜ'yeiletilecek.

…

ITU, OASIS ve ISO/IEC JTC 1/SC 27/WG 4, ITU-T Study Group 17'nin siber güvenlikalanında daha fazla standart işbirliğine nerede katkıda bulunabileceğini belirlemek amacıyla ilgili standardizasyon faaliyetlerine ilişkin içgörüyü paylaşacak.

"Tüm sanayi sektörleri ve kamu sektörü kuruluşları BİT'nin yardımıyla yenilikler yapmaktadır. Bu BİT her yerde siber güvenlik meydan yerçekimi artar," Heung Youl Youm, İTÜ-T Çalışma Grubu 17 Başkanı diyor. "Sınır ötesi ve önemli varlıkları hedef alan akıllı siber saldırılar, eşgüdümlü bir küresel tepki talep ediyor. İTÜ-T Çalışma Grubu 17 bu koordinasyonu teşvik ediyor." Bkz. INTERNATIONAL TELECOMUNICATION UNION, "28 August: ITU workshop on advanced cybersecurity attacks and ransomware", 16.08.2018, https%3a%2f%2fnews.itu.int%2f28-august-itu-workshop-on-advanced-cybersecurity-attacks-and-ransomware%2f, ET. 27 Şubat 2020. (Google translate ile çeviri yapılmıştır.)

596 Samet ve Aslan, a.g.e., s. 231.

597 EUROPOL, "CYBERCRIME", https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

598 Samet ve Aslan, a.g.e., s. 234.

599 "Bilgi çalan Zegost zararlı yazılımı, kişiye özel oltalama kampanyalarında bir dönüm noktası teşkil ediyor ve karmaşık yapıda teknikler kullanıyor. Tıpkı bilgi çalmayı amaçlayan diğer zararlı yazılımlar gibi Zegost'un da asıl amacı kurbanın cihazına ait bilgi toplamak ve bunları ele geçirmek. Ancak, bilgi çalmayı hedefleyen diğer yazılımlarla karşılaştırıldığında, Zegost, benzersiz bir şekilde fark edilmemek üzere yapılandırıldı. Örneğin; Zegost olay kayıtlarını temizlemek için tasarlanan bir işlevselliğe sahip. Tipik zararlı yazılımlarda, bu türden bir temizleme özelliği görülmüyor. Zegost'un atlatma yeteneklerindeki ilginç gelişmelerden biri de bulaşma rutinini başlatmasının ardından 14 Şubat 2019'a kadar bilgi çalma özelliğini "hareketsiz" tutan bir komuta sahip olmasıydı.

uzmanlık gerektiren bir konu olduğundan başlık altında ismen değinilmesinin konumuz açısından yeterli olacağı düşünülmektedir.[600]

1.2.5.4. Kritik Altyapılar

Bilişim suçlarının siber terörle anılmasının arttığı günümüzde devletler sanal ağlar tarafından oluşturulan "kritik altyapılar" ın (yerleşkelerin, ağların, servislerin veya yapıların) yok edilmesi veya işleyişinin aksatılmasının sağlık, kamu düzeni, güvenlik veya bireylerin ekonomik iyiliği, devletin fonksiyonlarının etkinliği üzerinde ciddi etki ve tehlikeleri olabileceği hususuna hassasiyet göstermeye başlamışlardır.[601]

Kritik altyapılar, ülkelerin ulusal düzeyde koruması gereken, sivil ve askeri saldırı ve tehditlere maruz kalabilen ve ülkeden ülkeye değişmekle birlikte çoğunlukla bankacılık, finans, enerji, ulaştırma, elektronik haberleşme, sağlık, su yönetimi, kritik kamu hizmetleri gibi sektörlerin altyapılarını ifade etmektedir.[602]

2016-2019 Ulusal Siber Güvenlik Strateji Belgesinin geneline bakıldığında, kritik altyapıların ulusal siber güvenliğin bir parçası olduğu[603] fikrinin yattığı açıkça görülmektedir. Nitekim, siber güvenliğin hedefi siber saldırıların yöneldiği bilişim sisteminin gösterdiği hizmetin korunması olup bu hizmetler kritik öneme haiz de olabilir.

Zegost'un ardındaki tehdit aktörleri, onu benzerlerine kıyasla daha uzun süreli bir tehdit haline getirerek, hedeflenen kurbanlarla bir bağlantı kurduğunu ve sürdürdüğünü garantilemek için bir dizi istismardan faydalanıyor." Bkz. CYBERMAG, "Siber Saldırganlar Yakalanmamak İçin Atlatma ve Anti Analiz Tekniklerine Yöneliyor", Sayı: 45, Ekim, 2019, ss. 26-27, s. 27.

600 Ayrıntılı bilgi için bkz. Samet ve Aslan, a.g.e., s. 234-249.

601 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 155.

602 Çiftçi, a.g.e. s. 13.

603 " "Kritik Altyapının Korunması" konulu Viyana Siber Güvenlik Haftası'nın üçüncü baskısı 11-15 Mart 2019 tarihleri arasında Avusturya'nın Viyana kentinde yapıldı.

Dünya Telekomünikasyon Geliştirme Konferansı 2017 (WTDC-17), Buenos Aires tarafından kabul edilen ITU Avrupa Bilgi ve İletişim Teknolojileri kullanımında Güveni ve Güveni Artırma Bölgesel İnisiyatifi çerçevesinde , Konferans Uluslararası Telekomünikasyon Birliği (ITU) Energypact Foundation ile baş koordinatör olarak görev yapıyor.

Bu beş günlük konferans, ulusal ve uluslararası paydaşları, dijital sistem koruması için riskler ve uygulama durumu hakkında bilgi alışverişi, güven oluşturma ve bilinçlendirme yapmak için kritik altyapı ve siber güvenlik alanında bir araya getirdi. Konferansın dört tematik baskısı vardı:

- Diplomasi - kritik altyapı koruması (CIP) ve siber güvenlik için uluslararası ve sınır ötesi konuları araştırmak
- Teknoloji - dijital dünyanın büyümesi ve dijital sistemlerin uygulanması ve korunmasının tartışılması
- İş dünyası - dijital dünyada iş risklerini, çözümlerini ve fırsatlarını inceleme
- Bilim - dijital sistem güvenliğinde mevcut Ar-Ge'yi sunmak" bkz. INTERNATIONAL TELECOMMUNICATION UNION, "Vienna Cyber Security Week 2019", https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/cybervienna.aspx, ET. 25 Şubat 2020. (Google translate ile çeviri yapılmıştır.)

Kritik altyapıların içeriği ülkeden ülkeye değişiklik göstermekte ise de bilgisayar ve iletişim ağlarını da kapsayacak şekilde genellikle açıkça tanımlanmış olup ABD' nin yayınlamış olduğu "Güvenli Siber Alan İçin Ulusal Strateji" belgesinde, sanal alanın "ülkenin kontrol sistemi" ve "siber alanın sağlıklı işleyişi ulusal güvenlik ve ulusal ekonomi için esastır" ifadeleri yer almış ve Birleşmiş Milletler Bilgi Toplumu Dünya Zirvesi' nde kritik bir internet kaynağı olan internet alan adları üzerindeki kontrolünü uluslararası yönetici bir yapıya devretmeyi de reddetmiştir.[604]

Avrupa Birliği kritik altyapıları, *'zarar görmesi veya yok olması halinde, vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik refahına veya kamu hizmetlerinin etkin ve verimli işleyişine ciddi boyutta olumsuz etki edebilecek fiziksel ve teknolojik tesisler, şebekeler, hizmetler ve varlıklar'*[605] olarak tanımlamış, 2016-2019 Ulusal Siber Güvenlik Strateji Belgesinde ise kritik altyapılar, *"İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır."*[606] şeklinde tanımlanmıştır. 2016-2019 Ulusal Siber Güvenlik Strateji Belgesinde "kritik altyapı sektörleri" ise **"**20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Kritik Kamu Hizmetleri", "Ulaştırma" ve "Bankacılık ve Finans" sektörleri"[607] olarak belirlenmiştir.

1.2.5.5. Siber Terörizm

Günümüzde bilgisayarların ve bilişim suçlarının terörizm ve organize suçlar olmak üzere iki önemli tehdit tarafından yönlendirilmekte olduğu bu bağlamda günümüz döneminde bireyselden ziyade toplumsal seviyedeki konuların ceza hukukunda yeni politikaların önemli hale gelmesi sonucunda "kritik altyapılar" dönemi olarak adlandırılabileceği belirtilmektedir.[608] Dijitalleşme sonucunda 21.

604 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 156.
605 European Union, "European Programme for Critical Infrastructure Protection", (Çevirimiçi) http://europea.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm 22 Şubat 2013 (*Aktaran* Çiftçi, a.g.e., s. 12).
606 T.C. ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s, 7.
607 A.e.
608 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 152.

Yüzyılın mermi ve bombalarının yerini bitler ve bytelar almış, toplumun sinir sistemini oluşturan bilişim sistemlerinin etkisizleştirilmesi, ülkelerin paralize hale getirilmesi anlamına gelmiştir.[609] Uluslararası alanda genel kabul gören bir tanımı mevcut bulunmayan ve siber alanın terörist faaliyetler için kullanılması sonucu ortaya çıkan "siber terör" kavramı bilgisayar ağlarını kullanarak kritik öneme sahip ulusal altyapılara (enerji, ulaşım ve devlet işlemleri) zarar vermeyi ya da tamamen kullanılamaz hale getirmeyi amaçlayan saldırılar biçiminde kendini göstermekte olup siyasal bir amaç uğruna insanlara zarar vermek veya acı çektirmek için devlet tarafından önemle korunan alanlardaki (telekomünikasyon, ulusal güvenlik ağları vs) bilgileri elde etmek, değiştirmek veya terörist amaçlar için kullanmak siber terörün önemli hedefleri arasında yer almaktadır.[610] Bu bağlamda öncelikle tanımlanması oldukça güç olan "terör" kavramını inceledikten sonra "siber terör" kavramını aydınlatmaya çalışacağız.

Genel geçer, tek tipte ve evrensel bir terör tanımında bulunmak zor bir iş[611] olmakla birlikte Birleşmiş Milletler Genel Konseyi tanımına göre "terör"[612];

> "*toplumda bir terör ortamı yaratmak maksadıyla; bir insan gurubu ya da belli insanlar tarafından siyasi amaçlarla girişilen ya da niyet edilen ve haklı görülmesini sağlamak için politik, felsefi ideolojik, ırkçı, etnik, dini ya da diğer kavramlar kullanılabilen; ancak hiçbir şart altında haklı görülemeyecek suç teşkil eden davranışlar."*[613] şeklinde,
>
> 12 Nisan 1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu' nda ise terör:
>
> "*cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki,*

"Ayrıca hukuka aykırı içerikler de hala suç politikasının gündeminde önemli bir yer işgal etmekte." Bkz. A.e.

609 A.e., s. 155.

610 Muharrem Gürkaynak ve Adem Ali İren, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, S:2, C:16, Yıl:2011, ss. 263-279. s. 266.

611 Bülent Tanör, "Terörle Mücade Kanunu Üzerine Düşünceler", MHB, Sayı: 1-2, Yıl:10, 1990, ss. 165-173, s. 166 https://cdn.istanbul.edu.tr/file/1CD58DF90A/3D3BD99CDB6C4BC2AAA65A1033855C78?, ET. 21 Şubat 2020.

612 "Terör terimi, dehşet ve korkuyu belirtirken terörizm, bu kavrama siyasi içerik ve süreklilik katmaktadır. Bu doğrultuda terörizm; "Savaş ve diplomasi ile kazanılmayan sonuçları elde etmek, korkutmak ve itaat ettirmek için bir teoriye, felsefeye ve ideolojiye dayanılarak siyasi maksatlarla, iradi olarak terör ve şiddetin sistemli ve hesaplı bir şekilde kullanılmasıdır" şeklinde tanımlanabilir." Bkz. Gizem Özkışlalı, *Küreselleşme, İnternet ve Terörizmin Değişen Yüzü: Siber Terörizm*, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı Yüksek Lisans Tezi, Ankara, 2008, s. 48, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

613 Bekir Peker, *Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Uluslar Arası İlişkiler Ana Bilim Dalı Yüksek Lisans Tezi, Konya, 2010, s. 35, 36, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

sosyal, laik, ekonomik düzeni değiştirmek, devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir."[614] olarak tanımlanmıştır.

Terörizmin ise, terör yöntemlerinin siyasi bir amaçla örgütlü, sistemli ve sürekli bir şekilde kullanılmasını benimseyen bir strateji olduğu dehşet ve korkuyu belirten "terör" kavramına süreklilik ve siyasal içerik kazandıran bir özelliği bulunduğu söylenebilmektedir.[615] 12 Nisan 1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu, üç ana terör suçu kategorisi öngörmekte olup birincisi, TCK' da yer alan bazı suçları içeren "terör suçları", ikincisi, TCK' da yer alan bazı suçların "terör amacı ile işlendiği takdirde terör suçu sayılanlar"ı ve üçüncüsü ise terör örgütlerini kurma faaliyetlerini düzenleme, yönetme veya bunlara girme suçlarından oluşmaktadır.[616]

Siber terör ve siber terörizm kavramı üzerinde anlaşma birliğine varılmış bir tanım bulunmamakta olup bunun ardında ise hemen hemen herkesin üzerinde uzlaşmış olduğu siber terimi ve 1793' den bu güne yaklaşık ikiyüzden fazla tanımı yapılmış "terör" kavramlarının bir araya gelmesi yatmaktadır. [617]

Siber uzay teknolojileri ve güvenlik uzmanı olan Prof. Dorothy E. Denning' e göre siber terörizm:

'Siber uzay ve terörizmin bileşimidir. Siber terör denince genellikle bilgisayarlara, ağlara ve buralarda saklanan bilgiye yöneltilen yasa dışı saldırı ve saldırı tehditlerinin siyasi ya da sosyal amaçlara ulaşmak için bir hükümet ya da çalışanlarına baskı yapmak ve gözdağı vermek maksadıyla yapılması anlaşılmaktadır. Daha da ötesi siber terörizm olarak tanımlanabilmesi için bir saldırının kişiler ya da mala karşı şiddetle sonuçlanması ya da en azından korku yaratacak kadar zarar verici olması gerekmektedir. Ölümle ya da yaralanma ile sonuçlanan saldırılar, patlamalar, uçak kazaları, su kirlenmeleri veya ciddi ekonomik kayıplar örnek olarak verilebilir. Kritik altyapı sistemlerine karşı yapılan saldırılar etkilerine bağlı olarak siber terörizm olarak

614 https://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf, ET. 21 Şubat 2020.
615 Peker, a.g.e., s. 36.
616 Tanör, a.g.e., s. 166, 167.
617 Peker, a.g.e., s. 40.

adlandırılabilir. önemsiz servisleri etkileyen saldırılar ve rahatsızlıklar siber terörizm olarak tanımlanamaz.'[618]

Yine bir başka tanımda ise "siber terör":

'Siyasi, sosyal ve ideolojik hedeflerin elde edilmesi maksadıyla; bir terör örgütü tarafından gerçekleştirilen, toplumda dehşet ve korku yaratan, hedefi bilişim sistemleri tarafından kontrol edilen kritik altyapı sistemleri veya bizzat kritik bilişim sistemleri, aracı ise yine bilişim sistemleri olan, etkisi bakımından klasik bir terör eylemine eşdeğer sonuçlar yaratan her türlü yasa dışı saldırı ve saldırı tehdidi dir.'[619] şeklinde tanımlanmıştır.

Uçakların kullandığı sistemlere yapılan saldırılar sonrasında rotada sapmaya yol açarak uçakların düşmesine neden olmak veya elektrik santrallerinin devreleriyle oynayarak uzun süreli elektrik kesintilerine neden olmak, acil servis ve polis imdat gibi hizmetlerin kullandığı çağrı merkezlerini tüm yurtta kullanılamaz hale getirerek halk arasında paniğe yol açmak, bankaların çok güvenli olarak bilinen sistemlerine girerek müşterilerin kimlik bilgilerini ve paralarını çalmak, siber teröre örnek olarak verilebilecek eylem türleridir.[620] Yine, gıda fabrikalarının üretim sürecini yöneten bilgisayar sistemlerinin ele geçirerek besin bileşenlerinin oranlarını değiştirilip bütün bir ulusun sağlığını tehdit edebilmesi, bankaların, uluslararası finans sistemlerinin ve borsa işlemlerinin çökertilerek vatandaşların ekonomik sisteme olan güvenlerinin kaybolmasına neden olabilme, gelecek nesil hava trafiği kontrol sistemlerine saldırarak yolcu uçaklarının çarpışmalarına, düşmelerine neden olabilme, ilaç üreten bir şirketin bilgisayarının ele geçirilerek ilaç bileşenlerinin değiştirilmesi suretiyle tahmin edilemeyecek sayıdaki insanın hayatını yitirmesine sebebiyet verebilme, bir şehrin trafik ışıklarını ya da metro trenlerine yön veren sinyalizasyon sistemine müdahale ederek kitlesel ölümlere yol açabilme, elektrik ve gaz nakil hatları, petrol boru hatları, barajlar vb. kritik birçok tesise karşı yıkıcı ve ölümcül saldırılar gerçekleştirebilmesi ihtimalleri veya senaryolarının da gerçekleşebilmesi olası siber terör eylemleri olduğu belirtilmektedir.[621]

618 Dorothy E., DENNING, "Cyberterrorism", (Çevirimiçi) http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html 20.08.2010 (*Aktaran* A.e., s. 38, 39)

619 Mesut Hakkı Caşın, *Uluslararası Terörizm*, Ankara, Nobel Yayın Dağıtım, 2008, s. 460 (*Aktaran* Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 174).

620 Gürkaynak ve İren, a.g.e., s. 267, 268.

621 Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 179, 180; Peker, a.g.e., s. 48.

Çağımızda terörizmin yeni bir yüzü olarak yansıyan siber terör ile birlikte savaşların ve terörizmin de şekli ve metodu yeni bir hal almış, klasik anlamdaki terör yerini evinde oturan, internet ve bilgisayarla ülkeleri ve savunma sistemlerine korku salan, siber saldırılara bırakmış, gerçekleştirilecek bir siber saldırı sonucunda bir barajın kapaklarının açabileceği, ordunun haberleşme sisteminin etkilenebileceği, kentin bütün trafik ışıklarını durdurulabileceği, telefonların felç edebileceği, elektrik ve doğalgazın kapatabileceği, bilgisayar sistemlerinin karmaşık hale getirebileceği, ulaşım ve su sistemlerinin çalışamaz hale getirilebileceği, bankacılık ve finans sektörünün çökertebileceği, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasının engelleyebileceği, hükümet kurumlarının alt üst edebileceği, sistemin birden durmasına neden olabileceği senaryo ve tehditleri öngörülebilir bir hal almaya başlamıştır.[622]

Siber terörizmi tanımlarken temelde terör olgusunun niteliklerinden ziyade terör olgusunun nasıl hayata geçirildiğinin önem arz etmekte olduğu, siber uzayda gerçekleştirilen eylemlerin, etki ve sonuçlarını gerçek dünyada hissettirdiği belirtilmektedir.[623] Bunun yanında siber terörün amacının devlet veya topluma yönelik mesajlar olduğu içerdiği, hedeflerinde şirketlerin, üçüncü şahısların ve finans kurumlarının olabileceği de vurgulanan başka bir noktadır.[624]

Siber terörizm ile terörizm arasında doğası gereği farklılıklar bulunduğu açıktır. Siber teröristlerin, klasik teröristlerin eylemlerini gerçekleştirirken ihtiyaç duyduğu bomba veya silahlara yerine sadece bir bilgisayar ve internet bağlantısına gereksinim duyması, giderek yaygınlaşan bilişim teknolojileri ile bu teknolojilerin kullanılırlığındaki artışın, herkesi potansiyel birer suçlu haline dönüştürebilmesi ve bunun sonucu olarak da terör örgütlerinin iş gördürme mantığıyla bilişim korsanlarını finanse edebilmesi, siber terörde insanların ölmesi ya da yaralanmasının şu an için söz konusu olmadığından kamuoyundan duygusal bir tepki doğması bakımından daha az olabileceği, klasik terör örgütlerinin, fiziki güç kullanımı sebebiyle elemanlarını en azından belirli bir yaşın üzerinde kişilerden seçmesi buna karşın siber terörde çocuk denecek yaştaki insanların siber terörün aracı haline gelebilmesi, klasik anlamdaki terör örgütlerinin eylem yaparken kendi hayatlarını da gerektiğinde ortaya koyma ihtimallerinin bulunmasına karşın siber terörizmde dünyanın herhangi bir yerinde

622 Peker, a.g.e., s. 41.
623 A.e., s. 40.
624 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 175.

internete bağlanan bir siber teröristin kendi yaşamını hiç tehlikeye atma riski bulunmadan istediği ülkenin toplumsal yaşamına ciddi zararlar verebilmesi gibi farklıların yanında asıl amacı gerçekleştirdiği fiiller ile hedef aldığı siyasal rejim ve topluma bir mesaj vermek başka bir deyişle şiddet ve zarar verme aracı olan pek çok klasik anlamdaki terörizm eylemlerinde terör örgütlerinin amaçlarının insan ölmesinden çok seslerini duyurmak olmasına rağmen siber terörizmde amaç ile aracın birbirine karıştığı, etkilerinin geniş bir kitleye yayıldığı ve çok yıkıcı olabildiği görülmektedir örneğin şehir su şebekesi sistemine, havalimanında kalkış ve uçuş sistemine borsada işlem gerçekleştirmeye olanak sağlayan sisteme veya bankaların bilişim sistemlerine girilerek ülke geneline verilecek zararın boyutu oldukça fazla olabilmektedir.[625]

Mukayeseli hukukta siber terörizm başlığı ile başlı başına bir yasa yer almamakta ise de gelişmiş ülkelerin terörizm yasalarında bu kavrama da yer verdikleri görülmekte, ülkemiz ceza mevzuatında ise siber teröre ilişkin özel bir yasa bulunmamakla birlikte Terörle Mücadele Kanunun 4'üncü m.' sinde 5237 sayılı TCK' nın 243. m.' sinde "Bilişim Sistemine Girme" suçu ile 244. m.' sindeki "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme" suçlarının 1'inci m.' de terör olarak sayılan amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlenmesi halinde terör suçu olarak değerlendirileceği hükme bağlandığı görülmektedir.[626] Şu an için büyük ve yakın bir terör tehdidinin algılanmadığı ancak bilişim teknolojilerindeki gelişmelerin her geçen gün büyük bir hız ve ivme içerisinde olduğu gerçeği karşısında ulusal bilgi altyapısı ve güvenliği oluşturulurken geleceğe yönelik bir bakış açısıyla hem teknik güvenlik önlemlerinin oluşturulmasında hem de yasal düzenlemelerde siber terör gerçeğinin şimdiden göz önünde bulundurulması gerektiği, ülkemiz mevzuatında ise ciddi bir tehdit olarak görülen siber terörizme ve bilişim sistemleri kullanılarak gerçekleşebilecek siber terörist eylemlere karşı yeterli düzenleme bulunmadığı, TCK' da ve özel yasalarda düzenlenen bilişim suçu tipleri incelendiğinde konuya dair en ufak bir düzenlemenin dahi bulunmadığı, siber terörizm olgusu dikkate alınarak veri iletim ağlarından yararlanılarak terör eylemlerinin gerçekleştirilmesinin ilgili suç tipi açısından cezayı artıran nitelikli hal sayılması gerektiği belirtilmektedir.[627] Ayrıca Avrupa Konseyi

625 Peker, a.g.e., s. 42-44.
626 Eryaman, a.g.e., s. 22.
627 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 181, 185.

Siber Suç Sözleşmesi' nde "siber terör" kavramına yer verilmemiş olunmasına rağmen Erdoğan, sistemlere müdahale fiilinin bilişim sistemleri ile kontrol edilen kritik altyapı tesislerine yapılması muhtemel fiilleri de kapsadığı bu bağlamda Sözleşme'de sistemlere müdahalenin suç olarak düzenlenmesi ile doğrudan ifade edilmese de "siber terör" fiillerine de uygulanabilir nitelikte olduğunu belirtmektedir.[628]

Kanaatimizce, yukarıda yer alan başlıklar altında ayrıntılı olarak incelendiği üzere bilişim teknolojilerinde yaşanan gelişmelerin geldiği nokta ve ilerleme hızı göz önünde bulundurulduğunda, siber güvenliğin önemi ve açık ve net siber terörizm tehdidinin varlığı yadsınamaz bir gerçektir. Ülkemiz açısından bakıldığında ulusal siber güvenliğin sağlanmasının ulusal güvenliğin bir parçası olarak görüldüğü bu bağlamda hem teknik olarak güvenliğin sağlanması hem de mevzuat açısından ciddi çalışmalar yapıldığı görülmektedir. Zira, güvenliğin geri planda bırakıldığı bir sistemin sonradan güvenli hale getirilmesinin daha zor olacağı ve istenilen ölçüde gerçekleştirilemeyeceği[629] açık olup bu bağlamda öncelikle veya eş zamanlı olarak suç öncesi güvenliğin sağlayacak düzenlemelerin, bir suçun varlığı halinde ise bununla en etkili biçimde mücadeleyi gerektiren hukuki altyapının oluşturulması bunun yanında da acil durumlara hızlı müdahaleye imkân sağlayan bir organizasyonel yapının varlığı[630] gerekmektedir. Nitekim, kritik sektörlerin belirlenmesi, bu sektörlerde yetkili kurumların sunulan kritik hizmetleri sağlayan işletmecilere yönelik güvenlik düzenlemeleri, servis sağlayıcılar tarafından tespit edilen siber olayların ulusal siber olaylara müdahale ekiplerine bildirilmesi gibi temel esaslara dayanan BTK tarafından yürütülen AB Şebeke ve Bilgi Güvenliği Direktifi' nin Uygulanmasına İlişkin AB ile Uyum Sağlanmasına Yönelik Teknik Yardım Projesi de ulusal mevzuatımızda yapılacak güncellemelere esas olması açısından siber güvenlik alanında yapılan ve güncel çalışmalara bir örnek oluşturmaktadır.[631] Siber güvenliğin ulusal güvenliğin bir parçası olduğunun kabulü karşısında ulusal ceza mevzuatımıza bakıldığında ise açık bir boşluk olduğu görülmektedir. Siber güvenlik, kritik altyapılar ve siber terörizm kavramlarının esasen birbirinden ayrılamaz kavramlar olduğu görülmektedir. Terör konusunda yıllardır ciddi yaralar almış bir ülke olarak değişen ve gelinen noktada siber

628 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 23.
629 Hekim ve Başıbüyük, a.g.e., s. 156.
630 A.e., s. 153.
631 BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, "Bakan Yardımcısı Sayan: Günümüzün En Önemli Konusu Dijital Ekonomi", 5.02.2020, https://www.btk.gov.tr/haberler/bakan-yardimcisi-sayan-gunumuzun-en-onemli-konusu-dijital-ekonomi, ET. 22 Şubat 2020.

terörizme dönüşen eylemlere karşı ceza hukuku anlamında da bir takım düzenlemeler yapılması gerektiği açıktır. Bu anlamda doktrinde yer alan bilişim sistemlerinden yararlanılması suretiyle terör eylemlerinin gerçekleştirilmesinin ilgili suç tipi açısından cezayı artıran nitelikli hal sayılması gerektiği fikrine katılmakla beraber TCK' nın onuncu bölümünde yer alan "Bilişim alanında suçlar" bölümü altında düzenlenmiş olan suç tipleri arasında mevcut hükümler arasında en uygun madde olduğu düşünülen 244. m.' ye 244/A şeklinde bir m. eklenerek (veya ileride yer alan bölümlerde de belirtileceği üzere 243 ile 244. m.' nin ortak bir m.' de birleştirilmesi sonucu yeni maddeye göre) kritik altyapıları hedef alan siber terör eylemlerinin ayrı bir suç olarak düzenlenebileceğini düşünmekteyiz. Bunun yanında 12 Nisan 1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu' nun "Terör suçları" başlıklı 3. m.' sine 2. fıkra olarak TCK' ya eklenmesini önerdiğimiz 244/A m.' si siber terör suçu olarak eklenerek TCK ile arasındaki bağlantının sağlanabileceği ayrıca "Cezaların artırılması" başlıklı 5. m.' ye de bilişim sistemlerinden yararlanılması suretiyle terör eylemlerinin gerçekleştirilmesi halinin cezayı artıran nitelikli hal olarak eklenmesi böylelikle çoklu ve tam bir koruma sağlanmasının yanında siber terör eylemi niteliğinde kabul edilebilecek eylemlerin ayrıca yaptırım altına alınması sonucunda caydırıcılık noktasında ileri bir aşamada kaydedilebileceği değerlendirilmektedir.

Yukarıda yer alan açıklamalarımıza ek olarak siber savaş, siber terör, siber silahlar gibi tanımların üzerinde ise küresel bir uzlaşı zor olsa da siber uzayın barışçıl kullanımı için uluslararası işbirliği, küresel standartlar ve normların oluşturulması, bir uzlaşı tesisi edilmesi için devletlerarası siber alana özgü geliştirilmiş ortak ve teknik bir dilin kullanımı, siber uzay alanı üzerinde devletlerarasındaki mücadelenin artması ile siber güvenlik konusunda uluslararası ilişkiler disiplinin ve güvenlik çalışmalarının analizi bunun yanında gerek uluslararası ve ulusal gerek kurumsal güvenlik açısından farklı disiplinleri içine alacak multidisipliner siber mücadele kavramı geliştirilerek bilimsel ve akademik literatüre katkıda bulunulması gerektiği de vurgulanması gereken başka bir nokta olduğu düşünülmektedir.

BÖLÜM II

BİLİŞİM SUÇLARINA İLİŞKİN MUKAYESELİ HUKUKTA YER ALAN DÜZENLEMELER VE YAPILAN ÇALIŞMALAR

Tek teknik standartlara dayanan ve küresel iletişime izin veren başka bir deyişle dünyanın her yerinden kullanıcılar tarafından erişilebilen İnternet hizmetlerinin (Facebook, Google, Yahoo ve diğerleri gibi) küreselleşmeye izin verme avantajına sahip olmasının yanında suç önleme perspektifinden bakıldığında, siber suç eylemlerinin suçlunun mağdurla aynı ülkede bulunmasını gerektirmemesi dezavantajına sahip olduğu, bunun da siber suç suçların büyük çoğunluğunun ulusötesi bir boyuta sahip olmasına sebebiyet verdiği görülmektedir.[632] Bu bağlamda siber suçların önlenmesi ve/veya bu suçlarla başarılı bir şekilde mücadele edilmesi, yeterli yasal araçların ve iyi eğitilmiş hükümet ve kolluk kuvvetlerinin aracılığıyla etkili uluslararası işbirliğini gerektirmektedir. Başka bir anlatımla, bugün için bilişim suçlarının uluslararası ceza hukukunun bir parçası olduğu, suçlarla etkin mücadele edilebilmesinin uluslararası boyutu ile düşünülmeksizin algılanamayacağı günümüzde yaygın bir görüş olarak benimsenmiş olup suçla mücadele noktasında uluslararası hukuksal düzenlemelerin oluşturulması, küresel ölçekte mevzuatın uyumlaştırılması özetle tüm dünyayı bir ağ şeklinde saran bilişim sistemlerinin ortaya çıkardığı bilişim suçları ile mücadelenin de dünya çapında bulunacak çözümlerle mümkün olduğu kabul edilmektedir.[633] Nitekim, bilişim dünyasının kendine has özellikleri ve bu dünyada işlenen suçların takibinin zorluğu uluslararası organizasyonların bünyesinde uluslararası işbirliğini ve devletlerin bir bütün olarak hareket etmelerini zorunlu hale getirmektedir.[634] Biz de çalışmamızın ikinci bölümünde öncelikle bazı uluslararası

632 UNODC, INTERNATIONAL TELECOMMUNICATION UNION, "Cybercrime : The Global Challenge", s. 1, 2, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf, ET. 28 Şubat 2020. (Google translate ile çeviri yapılmıştır.)
633 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 196.
634 Yaycı, a.g.e., s. 37.

kuruluşların yapmış olduğu çalışmalara değinerek Avrupa Konseyi üyesi ülkemizin de taraf olduğu bilişim suçları alanında ilk ve tek küresel belge niteliğinde olması sebebiyle Avrupa Konseyi Siber Suç Sözleşmesi' ni ayrıntılı olarak işledikten sonra bilişim suçlarının yabancı ulusal mevzuatlarda düzenlenmiş şekillerini belirttikten sonra ikinci bölümü tamamlayacağız.

2.1. BİLİŞİM SUÇLARINA İLİŞKİN ULUSLARARASI ÖRGÜTLERİN ÇALIŞMALARI

2.1.1. Birleşmiş Milletler

Birleşmiş Milletler bünyesindeki ilk çalışma 1985 yılında "7. Suçtan Korunma ve Suçluların Rehabilitasyonu Kongresi" olarak kendini göstermekte olup bu kongre sonrasında hazırlanan "Milan Eylem Planı" nın 224. paragrafında örnek olarak bilgisayar suçlarının gösterilerek yeni mağdur şekillerinin ortaya çıktığı ifade edilmiş, bilişim suçları ilk kez Milan Eylem Planı'nda tanımlanan suçlara karsı uluslararası eylem planının açıklandığı raporun 42 – 44. paragrafları arasında yer almış, 1990 yılında ise "8. Suçtan Korunma ve Suçluların Rehabilitasyonu" Kongresi Havana'da düzenlenmiş ve kongrenin ardından düzenlenen raporda ise bilgisayar bağlantılı suçlara özel bir bölüm verilerek birtakım tavsiyelerde bulunulmuştur.[635] Yine, Birleşmiş Milletler tarafından 2000 yılında düzenlenen "Sınır Ötesi Organize Suçlarla Mücadelenin Önemine İşaret Edilmesi" sempozyumunda üye ülkelere, bilgisayar sistemlerine yetkisiz giriş, bilgisayar veya bilgisayar sistemlerinin hukuka uygun kullanılmasına engel olunması, bilgisayar sistemleri içerisindeki verilerin yok edilmesi veya değiştirilmesi, gayri fiziki ekonomik değer taşıyan objelerin çalınması ve aldatma yoluyla değer elde edilmesi eylemlerinin cezai yaptırım altına alınması önerilmiştir.[636] Ayrıca, Birleşmiş Milletler nezdinde Siber suçlara dair Hükümetlerarası Uzmanlar Grubu da kurulmuş ve ilk toplantısını 2011'de gerçekleştirmiştir.[637]

Birleşmiş Milletler' in siber güvenlik alanında "Bilişim teknolojilerinin kötüye kullanılması ile mücadele" konulu 55/63 sayılı ve Ocak 2001 tarihli kararı, "Bilgi teknolojilerinin cezai kullanımıyla mücadele" konulu 56/121 sayılı ve Ocak 2002 tarihli kararı, "Küresel bir siber güvenlik kültürünün oluşturulması" konulu 57/239

635 Karagöz, a.g.e., s. 86, 87; Yaycı, a.g.e., s. 41.
636 Eker, a.g.e., s. 109, 110.
637 Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesı Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", Prof. Dr. Nur Centel' e Armağan, ss. 1229-1269, s. 1239, http://dosya.marmara.edu.tr/huk/fak%C3%BCltedergisi/nurcentel/muratonok.pdf, ET. 1 Mart 2020.

sayılı Ocak 2003 tarihli kararı, "Küresel bir siber güvenlik kültürünün oluşturulması ve kritik bilgi altyapılarının korunması" konulu 58/199 sayılı Ocak 2004 tarihli kararı ve "Küresel bir siber güvenlik kültürünün oluşturulması ve kritik bilgi altyapılarının korunması için ulusal çabaların değerlendirilmesi" konulu 64/211 sayılı Mart 2010 tarihli kararı bulunmaktadır.[638]

İlk olarak uluslararası telgraf ağlarını yönetmek için 1865 yılında kurulan, bilgi ve iletişim teknolojilerine ulaşılabilirlik, yapay zeka, genişbant, çevre ve iklim değişikliği, siber güvenlik vb.[639] temel faaliyet alanları bulunan International Telecommunication Union (ITU) , Birleşmiş Milletler' in bilgi ve iletişim teknolojileri konusunda uzmanlaşmış ajansıdır.[640] ITU' nun siber güvenlik ve siber suçla ilgili yetkisi, Tam Yetkili Konferanslar ve dünya meclisleri gibi resmi kurumsal toplantılarda alınan kararlara dayanmakta olup özellikle "Tam Yetkili Karar 130 (Rev. Guadalajara, 2010)", ITU' nun siber güvenlik ve siber suçlar üzerindeki rolünü güçlendirerek, Genel Sekretere ve ITU Bürolarının Direktörlerine, belirli gelişmekte olan ülkelerde üye devletlere, uygun ve uygulanabilir hukukun hazırlanmasında yardımcı olmaları konusunda talimat vermiştir.[641] ITU' nun siber güvenlik alanında birçok çalışması ve kararı bulunmakta[642] olup bunun yanında "Siber suç mevzuatını yürürlüğe koymayı ve yürürlüğe koymayı amaçlayan faaliyetleri koordine etmek için yasal bir strateji için pratik rehberlik" başlıklı ITU-T SG 17 (Çalışma Dönemi 2013) Katkı 340 belgesi[643], "Siber suçla teknik yollarla mücadele hakkında yeni soru için önerilen metin" başlıklı ITU-T SG17 (Çalışma Dönemi 2005) Geçici Belge 2779-WP2 belgesi[644], "Bangladeş'te siber suçun önlenmesi" başlıklı ITU-D SG01 Katkısı 203

638 Ayrıntılı bilgi için bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx, ET. 27 Şubat 2020.
Ayrıntılı bilgi için bkz. UNITED NATIONS, "Birleşmiş Milletler Dijital Kütüphanesi", https://digitallibrary.un.org/, ET. 28 Şubat 2020.
639 Bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/action/Pages/default.aspx, ET. 26 Şubat 2020.
640 Ayrıntılı bilgi için Bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/history/Pages/DiscoverITUsHistory.aspx, ET. 26 Şubat 2020; INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/about/Pages/default.aspx, ET. 26 Şubat 2020.
641 "Cybercrime : The Global Challenge", s. 4.
642 Kararlar için bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/action/cybersecurity/Pages/itu-resolutions.aspx, ET. 27 Şubat 2020.
643 Bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/md/T13-SG17-C-0340, ET. 27 Şubat 2020.
644 Bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/md/T05-SG17-070919-TD-WP2-2779, ET. 27 Şubat 2020.

belgesi[645] gibi rapor ve belgeler de yayınlamaktadır. Siber tehditlere karşı korunma ile ilgili ITU' nun 2007 yılında somut tepkisi olan Global Cybersecurity Agenda (Küresel Siber Güvenlik Gündemi) "GCA"[646] ise, Bilgi ve İletişim Teknolojileri (BİT) kullanımında küresel halkın güvenini ve güvenliğini artırmayı amaçlayan uluslararası işbirliği için küresel bir çerçevedir.[647] ITU yine, büyüyen siber tehditlerin ulusal ve uluslararası etkilerinin anlaşılması, ülkelerin mevcut ulusal bölgesel ve uluslararası belgelerin gereksinimlerini değerlendirmeleri, siber güvenliğin yasal yönlerini anlamaları, yasal çerçevelerin uyumlaştırılması ve sağlam bir yasal temel oluşturmaları hususlarında yardımcı olmayı amaçlayan Siber Suç Kılavuzu' nu (Siber Suç Mevzuatı Kaynağı/ ITU Cybercrime Legislation Resources) yayınlamıştır.[648]

---

645 Bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/md/D10-SG01-C-0203, ET. 28 Şubat 2020.

646 "11 yıl önce, 2007 yılında, zamanın İTÜ Genel Sekreteri Dr. Hamadoun I. Touré (2007 -2014) tarafından başlatılan İTÜ Küresel Siber Güvenlik Gündemi (GCA), bilgi toplumunda güven ve güvenliği artırmayı amaçlayan uluslararası işbirliği çerçevesidir. GCA, işbirliği ve verimlilik için tasarlanmıştır, ilgili tüm ortaklarla işbirliğini teşvik eder ve yineleme çabalarını önlemek için mevcut girişimleri geliştirmeyi teşvik eder.
GCA, Child Online Protectiongibi girişimleri teşvik etmiştir ve tüm paydaş gruplarından önde gelen küresel oyuncuların desteğiyle, dünya ülkelerine siber güvenlik çözümleri dağıtmaya devam etmektedir.
GCA, çalışma alanları olarak da bilinen aşağıdaki beş stratejik sütun üzerine inşa edilmiştir:

- Yasal Önlemler
- Teknik & Usul Önlemleri
- Organizasyon Yapıları
- Kapasite Geliştirme
- Uluslararası İşbirliği" Ayrıntılı bilgi için bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx, ET. 28 Şubat 2020. (Google translate ile çeviri yapılmıştır.)

647 "Siber suç da dahil olmak üzere siber güvenliğin yasal ve yaptırımla ilgili yönleri bir dizi çalışma grubunda ve Kalkınma sektörü (ITU-D) tarafından düzenlenen çeşitli bölgesel konferanslarda ele alınmıştır. ITU / AB ortak finansmanlı bir projede, ITU, çeşitli Asya, Karayipler ve Pasifik ülkeleri için siber suçlarla ilgili yasal çerçevelerin iyileştirilmesi ve kapasite geliştirme konusunda ülke içi yardım sağlamaktadır. Örgüt ayrıca, siber suç eğitim kursları ve polis, hakimler, avukatlar ve sivil toplum için ilgili eğitim materyalleri gibi araçlar da geliştirmiştir. Buna, tüm BM dillerinde ücretsiz olarak sunulan siber suçlarla ilgili kapsamlı bir yayın da dahildir." Bkz. Cybercrime : The Global Challenge, s. 4, (Google translate ile çeviri yapılmıştır.)

648 "Rehber altı ana bölüm içermektedir. Girişten sonra (Bölüm 1), Rehber siber suç olaylarına genel bir bakış sunmaktadır (Bölüm 2). Bu, suçların nasıl işlendiğine dair açıklamaları ve bilgisayar korsanlığı, kimlik hırsızlığı ve hizmet reddi saldırıları gibi en yaygın siber suç suçlarının açıklamalarını içerir. Rehber ayrıca siber suçların soruşturulması ve kovuşturulmasıyla ilgili zorluklara ilişkin bir genel bakış sunmaktadır (Bölüm 3 ve 4). Uluslararası ve bölgesel kuruluşlar tarafından siber suçlarla mücadelede yürütülen bazı faaliyetlerin bir özetinin ardından (Bölüm 5), Kılavuz, maddi ceza hukuku, usul hukuku, uluslararası işbirliği ve sorumluluğunun farklı hukuksal yaklaşımlarının analiziyle devam etmektedir. İnternet Servis Sağlayıcıları (Bölüm 6), uluslararası yaklaşımların örneklerini ve ulusal çözümlerden iyi uygulama örneklerini içerir. ülkelere uyumlaştırılmış siber suç yasaları ve usul kurallarının oluşturulmasında yardımcı olabilecek örnek yasal dil ve referans materyalleri sağlamayı amaçlamaktadır." Bkz. INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html, ET. 28 Şubat 2020. (Google translate ile çeviri yapılmıştır.)

Birleşmiş Milletler Uyuşturucu ve Suç Ofisi, (United Nations Office on Drugs and Crime) (UNODC) Birleşmiş Milletler Uluslararası Uyuşturucu Kontrol Programı (UNDCP) ile Suç Önleme ve Ceza Adaleti Bölümlerinin 1997 yılında Viyana'da Birleşmiş Milletler Ofisinde birleştirilmesi neticesinde yaşadışı uyuşturucu ticareti suçlarınının önlenmesi ile mücadele, uluslararası terörizm ve siyasi yolsuzluklar konularında birbirleriyle koordineli ve kapsamlı çalışmalar yapılması ve suçlara çözüm bulmada Birleşmiş Milletlere yardımcı olması amacıyla kurulan ve 2002 yılından itibaren Birleşmiş Milletler Uyuşturucu ve Suç Ofisi olarak yeniden adlandırılan bir ofis olup uzun vadeli amaçları arasında, hükümetlere bağlı kamu kurum ve kuruluşları arasında uyuşturucu madde, suç, terörizm ve yolsuzluk ile ilgili konularda küresel olarak paylaşılan bilgileri en üst seviyeye çıkartmak ve kamuoyunda bu konularda küresel, ulusal ve toplumsal düzeyde farkındalık yaratmak yer almaktadır.[649] Bunun yanında UNODC, ulusal yapıları ve eylemi destekleyerek siber suçlarla mücadelede uzun vadeli ve sürdürülebilir kapasite oluşturmayı teşvik etmektedir.[650] UNODC Genel Kurul'dan gelen bir görev gereği siber suç sorunu ve buna verilen yanıtlar hakkında kapsamlı bir çalışmalar yürütmekte çeşitli el kitapları ve çalışmalar yayınlamakta ve bu konularla ilgili çalışmalara katkıda bulunmaktadır.[651] Bu bağlamda, UNODC Suç Önleme ve Ceza Adaleti Komisyonu (CCPCJ) 2015 yılında ülkelere siber suçluları önleme ve etkili bir şekilde kovuşturma çabalarında yardımcı olmayı amaçlayan mevzuat, içtihat ve siber suç ve elektronik kanıtlar la ilgili merkezi bir veri tabanı olan "siber suç deposu" nu başlatmıştır.[652] Bunun dışında, Birleşmiş Milletler Genel Kurul'unun 65/230 sayılı kararı gereği, UNODC Suç Önleme ve Ceza Adaleti Komisyonu' nun (CCPCJ) 22/7 ve 22/8 kararlarına göre üye devletlere kapasite geliştirme ve teknik yardım yoluyla siber suçlarla mücadelelerinde yardımcı olmakla görevli Siber Suçlar Küresel Programı kabul edilmiştir.[653]

649 https://tr.wikipedia.org/wiki/Birleşmiş_Milletler_Uyuşturucu_ve_Suç_Ofisi, ET. 28 Şubat 2020.
650 Ayrıntılı bilgi için bkz. UNODC, https://www.unodc.org/, ET. 28 Şubat 2020.
651 "Cybercrime : The Global Challenge", s. 3.
652 UNODC, https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html, ET. 28 Şubat 2020.
653 UNODC, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html, ET. 28 Şubat 2020.

2.1.2. OECD (Organisation for Economic Cooperation and Development - Ekonomik Kalkınma ve İşbirliği Örgütü)

14 Aralık 1960 tarihinde imzalanan Paris Sözleşmesi' ne dayanılarak, 1961' de kurulmuş olan Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Co-operation and Development - OECD)[654] ekonomik büyüme, mali istikrar, ticaret ve yatırım, teknoloji, yenilik, girişimcilik ve kalkınma alanlarında işbirliği ile üye ülkelere yardımcı olma amacı güden uluslararası bir ekonomi örgütü olup Türkiye birliğin 20 kurucu üyesi arasında yer almaktadır.[655]

O.E.C.D. bünyesinde, uluslararası alanda karşılaştırılmalı olarak bilişim suçları ile ilgili ceza yasalarının birbirleriyle uyumlaştırması çalışmaları, 1983 yılında başlatılmış ve 1986 yılında yayınlanan "Bilgisayarla İlgili Suç: Hukukî Politikaların Analizi - Computer Related Crime: Analysis of Legal Policy" raporu ile somutlaşarak rapor ile üye ülkelere; bilgisayar yoluyla dolandırıcılık, bilgisayar yoluyla sahtecilik, bilgisayar program ve verilerinde değişiklik yapılması, bilgisayar programlarının telif haklarına aykırı olarak kopyalanması, çoğaltılması ve dağıtılması, telekomünikasyon sistemlerinin, bilgisayarın diger fonksiyonlarının ve iletişimin değişikliğe uğratılması gibi ihlalleri cezai müeyyide ile karşılamaları önerilmiştir.[656] Yine OECD' nin 1992 yılında yayınlamış olduğu bir başka raporunda ise, bilinç, sorumluluk, tepki, etik, demokrasi, risk değerlendirmesi, güvenlik tasarımı ve uygulama, güvenlik yönetimi ve yeniden değerlendirme başlıkları ile dokuz tane ilke üye ülkelere yön gösterecek şekilde önerilmektedir.[657] 1997 ve 2002 yıllarında, hazırlanan tavsiye örgüt tarafından tekrar gözden geçirilerek 2007 yılında ise tavsiyenin anılan 2002 versiyonu birinci kez, 2012 yılında ise, ikinci kez gözden geçirilerek güncellenmiştir.[658] 2002 yılında ise

654 https://tr.wikipedia.org/wiki/OECD, ET. 29 Şubat 2020.
655 T.C. DIŞİŞLERİ BAKANLIĞI, http://www.mfa.gov.tr/iktisadi-isbirligi_ve-gelisme-teskilati-_oecd_.tr.mfa, ET. 29 Şubat 2020.
656 Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", s. 2752; Eker, a.g.e., s. 109; Yaycı, a.g.e., s. 40.
Ayrıntılı bilgi için bkz. OECD, https://www.oecd-ilibrary.org/, ET. 29 Şubat 2020.
657 Ayrıntılı bilgi için bkz. OECD, https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm, ET. 29 Şubat 2020. (Google translate ile çeviri yapılmıştır.)
Raporun Türkçe metni için bkz. OECD, https://www.oecd.org/sti/ieconomy/32493366.PDF, ET. 29 Şubat 2020.
OECD' nin yayınlamış olduğu "Bilgisayar Virüsleri ve Diğer Kötü Amaçlı Yazılımlar" adlı rapor ve "Çevrimiçi Kimlik Hırsızlığı" raporu için bkz. OECD, https://www.oecd-ilibrary.org/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en, ET. 29 Şubat 2020; OECD, https://www.oecd-ilibrary.org/science-and-technology/online-identity-theft/the-scope-of-online-identity-theft_9789264056596-3-en, ET. 29 Şubat 2020.
658 Akpek, a.g.e., s. 12.

OECD Konseyi tarafından "Bilgi Sistemleri ve Ağlarının Güvenliği İçin OECD Rehber İlkeleri: Güvenlik Kültürüne Doğru" adlı belge kabul edilmiştir.[659]

2.1.3. G8 (Group of Eight- Sekizler Grubu)

Sekizler Grubu (Group of Eight- G8), Kanada, Fransa, Almanya, İtalya, Japonya, Rusya, Birleşik Krallık ve ABD gibi dünya ekonomisinin yaklaşık %65' ini temsil eden üye ülkelerden oluşan bir uluslararası hükümetler forumu olup yıl boyunca konferanslar ve politik araştırmalar yapmakta, 1975' ten beri yıllık ekonomi zirveleri düzenlemekte[660] bunun yanında bilişim suçları alanında da birtakım çalışmalar gerçekleştirerek raporlar yayınlamaktadır.

G8, 1995 yılında Kanada'da düzenlenen toplantısında, liderler, "Lyon Grubu" olarak anılan "Organize Suçlar Kıdemli Uzmanlar Grubu" nun (Senior Experts Group on Organized Crime) oluşturulmasına karar vermiş, "Lyon Grubu" aynı yıl "Ülkelerarası Organize Suçlarla Etkin Mücadelede Tavsiyeler" adı altında uluslararası organize suçlarla mücadele konusunda bir rapor yayınlamış, 1997 yılında G7 bünyesinde ise, "İleri Teknoloji Suçları Alt Komitesi" oluşturulmuş ayrıca soruşturma ve kovuşturma işlemlerini kolaylaştırmak ve bunun yanında bilişim suçları konusunda dijital kanıtların ele geçirilmesi ve saklanabilmesi amacıyla da "24 saat hizmet veren bir iletişim grubu" oluşturulmuştur.[661] 1997 yılında ise G8 "İleri Teknoloji Suçları" üzerinde "10 Prensip ve 10 Noktada Eylem Planı" üzerine anlaşmaya varmış, bu bağlamda 18 Mayıs 1998' de İngiltere'de yapılan zirvede, söz konusu prensipleri içeren bildiri liderler tarafından imzalanarak bildiri Aralık ayında yayımlanmıştır.[662] Bu durumun, G8 bünyesinde yaratılan ve uluslararası işbirliği açısından temel bir referans oluşturup, Budapeşte Sözleşmesi'nin 35. m.' sinde de yansımasını bulan "Contact Points Network" anlayışını oluşturduğu belirtilmektedir.[663] G8' in 2000 yılında Japonya'da düzenlemiş olduğu zirvede, OECD Bilgi Güvenliği Rehberi'ne uygun gerekli politika ve tedbirlerin uygulanmasının gerekliliğinin vurgulanarak Okinava Küresel Bilgi Toplumu Bildirisi ortaya konulmuş, bildiri ile siber suçlardan arınmış daha güvenli bir siber uzay kararlılığını vurgulamış bu kapsamda, üye

659 Önok, a.g.e., s. 1240.
660 https://tr.wikipedia.org/wiki/G8, ET. 29 Şubat 2020.
661 Yaycı, a.g.e., s. 38; Karagöz, a.g.e., s. 90.
662 Yaycı, a.g.e., s. 38, 39; Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", s. 2753.
663 Önok, a.g.e., s. 1240, 1241.

devletlere Avrupa Konseyi Siber Suçlar Sözleşmesine taraf olunması için çağrıda bulunularak üye devletlerden uluslararası örgütlerin bu yönde vermiş olduğu tavsiyelere uyulması istenmiştir.[664]

2.1.4. Interpol, Europol, Eurojust

1923 yılında uluslararası polis işbirliği sağlamak amacıyla kurulan ve tüm dünyanın ortak birimi olan INTERPOL (*International Criminal Police Organization* - Uluslararası Kriminal Polis Teşkilatı), Birleşmiş Milletler' den sonra, dünyanın ikinci büyük uluslararası örgüttür.[665] Interpol, uluslararası siber suç operasyonlarını yerinde veya uzaktan koordine ederek birden fazla ülkeyi kapsayan şüphelileri, kurbanları ve suçları içerebilecek siber suç olaylarında üye ülkelerin soruşturma yürütmelerine yardımcı olmakla birlikte polisin eylemlerini yönlendirmek için en güncel tehdit bilgilerine sahip olmasını da sağlayarak eğitimler düzenlemekte[666] bunun yanında siber suçlar konusunda diğer kuruluşlarla ortaklıklar, gerçekleştirerek üye ülkelerin kamu, özel ve akademik sektörlerindeki siber ve teknolojik uzmanlıktan yararlanmalarını sağlamakta, yeni ortaya çıkan siber tehditler hakkında bilgi alışverişinde bulunmaktadır.[667]

2016 yılında INTERPOL ve Nijerya Ekonomik ve Mali Suçlar Komisyonu arasında gerçekleştirilen ortak operasyonda çevrimiçi dolandırıcılık şebekesinin arkasındaki elebaşını tutuklamış, ASEAN operasyonunda, çeşitli kötü amaçlı yazılım türlerini yayan komut ve kontrol sunucularını belirlemek için polis ve özel sektörün uzmanlığını birleştirerek hükümet portalları da dahil olmak üzere güvenliği ihlal edilmiş yaklaşık 270 web sitesinin keşfedilmesini sağlamıştır.[668]

Terörizm, organize suçluluk ve diğer ağır suçların önlenmesi ve bunlarla mücadelede üye ülkeleri desteklemek ve işbirliğini sağlamak amacıyla kurulan ve

664 Akpek, a.g.e., s. 14.
665 https://tr.wikipedia.org/wiki/Interpol, ET. 2 Mart 2020.
666 INTERPOL, https://www.interpol.int/Crimes/Cybercrime/Our-cyber-operations, ET. 2 Mart 2020; INTERPOL, https://www.interpol.int/Crimes/Cybercrime/Investigative-support-for-cybercrime, ET. 2 Mart 2020.
667 Ayrıntılı bilgi için bkz. INTERPOL, https://www.interpol.int/Crimes/Cybercrime/Cyber-partnerships, ET. 3 Mart 2020.
668 " 'Siber dalgalanma' operasyonlarımız, özel sektör ortaklarıyla geliştirilen tehdit bilgileri üzerinde hareket etmek için araştırmacıları bir araya getiriyor. Bunlara 2017 yılında ASEAN (Güneydoğu Asya) ve Amerika kıtası dahil edildi." Bkz. INTERPOL, https://www.interpol.int/Crimes/Cybercrime/Our-cyber-operations, ET. 2 Mart 2020. (Google translate ile çeviri yapılmıştır.)

Avrupa Birliği (AB) kuruluşu niteliğinde olan[669] "EUROPOL"[670] (European Police Office - Avrupa Polis Teşkilatı) tarafından Avrupa çapındaki sınır aşan siber suçların soruşturulmasında eşgüdümü sağlama amacı güden "High Tech Crime Centre"'ın (Yüksek Teknolojili Suçlar Merkezi) kurulmuş olup 2010 yılında ise EUROPOL içinde Avrupa Komisyonu, EUROJUST ve AB ülkelerinin siber suçlulukla mücadele birimlerinin başındaki kişilerden oluşan AB içinde uyumlu bir yaklaşımın geliştirilmesinde ve teşvikinde yardımcı olmak ve suç işlemekte siber teknolojinin kullanımından kaynaklanan sorunlara cevap bulmak amacı güden "European Cybercrime Task Force (EUCTF)"[671] (Avrupa Siber Suç Görev Timi/Gücü) adlı bir platform kurulmuştur.[672] Europol tarafından 2013 yılında ise "Avrupa Siber Suçlar Merkezi – European Cybercrime Centre (EC3)"[673] kurulmuş olup bu merkez adli tıp, strateji ve operasyonlar olmak üzere siber suçlarla mücadelede üç yönlü yaklaşım benimsemekte ve her yıl "İnternet Organize Suç Tehdidi Değerlendirmesi – Internet Organised Crime Threat Assessment" "(IOCTA)"[674] stratejik raporunu

669 Ayrıntılı bilgi için bkz. Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* s. 85, dipnot. 270.

670 Avrupa Birliği' nin kolluk kuvveti niteliğinde olan Europol, 27 AB Üye Devletini terörizm, siber suç ve diğer ciddi ve organize suç biçimlerine karşı mücadelelerinde desteklemenin yanında ayrıca AB üyesi olmayan birçok ortak ülke ve uluslararası kuruluşla da çalışmaktadır. Ayrıntılı bilgi için bkz. EUROPOL, https://www.europol.europa.eu/about-europol, ET. 1 Mart 2020.

671 Ayrıntılı bilgi için bkz. EUROPOL, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf, ET. 1 Mart 2020.

672 Önok, a.g.e., s. 1241; Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 78, dipnot. 245.

673 "…Siber suçları ele almak için kolluk yöntemlerinin, siber suçlular tarafından kullanılanlardan daha fazla olmasa da, daha karmaşık olması gerekir. EC 3 , organize suç grupları tarafından yürütülen yasadışı çevrimiçi faaliyetlere, özellikle e-bankacılığı ve diğer çevrimiçi finansal faaliyetleri, çevrimiçi çocuk cinsel sömürüsünü ve AB'deki kritik altyapıyı ve bilgi sistemlerini etkileyen suçları ele alacak.
Üye Devletlerdeki görevlerini yerine getirmek ve siber suç araştırmacıları, savcıları ve hakimleri daha iyi desteklemek için, EC 3 açık kaynaklardan, özel sektörden, polis ve akademiden gelen bilgileri kaynaştıracaktır. Yeni Merkez ayrıca, Avrupa Siber Suç uzmanlığı ve eğitim çabalarını bir araya getiren ve ortaklardan gelen belirli teknik ve adli konulardaki sorulara cevap veren AB Üye Devletlerindeki ulusal polis için bir bilgi tabanı görevi görecek…" bkz. EUROPOL, https://www.europol.europa.eu/newsroom/news/media-invitation-to-opening-of-european-cybercrime-centre-ec3-europol, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

674 Ayrıntılı bilgi için bkz. EUROPOL, https://www.europol.europa.eu/iocta/2017/THE_GEOGRAPHIC_DISTRIBUTION_OF_CYBER CRIME.html, ET. 1 Mart 2020.
"EC3 her yıl, o yıl için odak noktası olan siber suç alanlarında EMPACT Operasyonel Eylem Planı için öncelikler belirleyen, yukarıda belirtilen İnternet Organize Suç Tehdidi Değerlendirmesi'ni (IOCTA) yayınlamaktadır." Bkz. EUROPOL, "CYBERCRIME", https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

yayınlamaktadır.[675] Türkiye ile Europol arasında teknik ve stratejil iş birliğine imkan tanıyan Türkiye Cumhuriyeti ve Avrupa Polis Teşkilatı Arasında İş Birliği' ne İlişkin Anlaşma imzalanarak 28 Temmuz 2004' te yürürlüğe girmiştir.[676] Europol tarafından yayınlanan birçok rapor bulunmakta olup 2018 yılı "İnternet Organize Suç Tehdidi Değerlendirmesi Raporu" siber saldırıları vurgulaması, yeni teknolojik gelişmeleri açıklaması bu bağlamda siber suçlarla mücadele konularında önemli incelemeleri içermektedir.[677] Europol ve Interpol tarafından 2013 yılında başlatılan ve her yıl düzenlenen Siber Suçlar Konferansı gerçekleştirilmektedir.[678] Bunun dışında Europol

675 Bkz. EUROPOL, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, ET. 1 Mart 2020.

676 Emniyet Genel Müdürlüğü bünyesinde Interpol-Europol Dairesi Başkanlığı ise bu kapsamda faaliyet göstermektedir. Bkz. Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 78, dipnot. 245.

677 "Rapor her yıl eşi görülmemiş bir kapsam ve ölçekte siber saldırıları vurgular. Bu yıl farklı değil, Europol misyonunun tam kalbinde bir kolluk olan kolluk camiamız içinde daha fazla işbirliği ve işbirliğine ihtiyaç olduğunu gösteriyor. Rapor aynı zamanda telekomünikasyon sahtekarlıkları gibi daha önce hafife alınan tehditlerin dikkatini gündeme getiriyor ve kolluk kuvvetlerinin sürekli adapte olması ve gelişmesi gerektiğini ve siber suçların her alanında sürekli eğitim ihtiyacını ortaya koyuyor.

Bazı siber saldırılar büyüklükleri ile manşetlere devam etse de, siber suçun diğer alanları daha az tehdit veya endişe kaynağı değildir. Ödeme sahtekarlığı, önemli mali kayıpları, suç kazançlarını ve diğer suçların kolaylaştırılmasını vurgulamaya devam etmektedir; çevrimiçi çocuk cinsel sömürüsü internetin en kötü yönlerini özetlemekte ve çocuklarımızı istismar etmek ya da kötüye kullanmak isteyenler için mevcut tehlikeyi vurgular.

Bu yılki raporda ayrıca Genel Veri Koruma Yönetmeliği (GDPR), Ağ ve Bilgi Güvenliği (NIS) yönergesi ve 5G teknolojisi gibi bazı önemli yasal ve teknolojik gelişmeler açıklanmaktadır. Bu gelişmeler olumlu olmakla birlikte, hepsi bir şekilde kolluk kuvvetleri olarak siber suçları etkin bir şekilde inceleme yeteneğimizi etkileyecektir. Bu, toplumumuzun nasıl geliştiğini dile getirmek için kolluk kuvvetlerinin politika yapıcılar, yasa koyucular ve endüstri ile ilişki kurma gereğini vurgulamaktadır." Bkz. EUROPOL, https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

678 Bkz. EUROPOL, https://www.europol.europa.eu/newsroom/news/5th-europol-interpol-cybercrime-conference-successfully-ends-record-participation-and-concrete-steps-for-future, ET. 1 Mart 2020.

6. Konferans ise 2018 yılında Singapur' da gerçekleştirilmiştir. Bkz. EUROPOL, https://www.europol.europa.eu/events/6th-interpol-europol-cybercrime-conference, ET. 1 Mart 2020.

Europol ve Eurojust , siber suçlarla mücadeledeki mevcut gelişmeleri ve ortak zorlukları tanımlayan ve kategorize eden üçüncü ortak raporu 5 Temmuz 2019' da yayınmıştır. Buna göre:

"Veri kaybı: elektronik veriler tüm siber suç alanlarında başarılı soruşturmaların anahtarıdır, ancak bu tür verileri elde etme olanakları önemli ölçüde sınırlandırılmıştır.

Yer kaybı: son eğilimler, kolluk kuvvetlerinin artık failin fiziksel yerini, ceza altyapısını veya elektronik kanıtları oluşturamayacağı bir duruma yol açmıştır.

Ulusal yasal çerçevelerle ilgili zorluklar: AB Üye Devletlerindeki yerel yasal çerçevelerdeki farklılıklar, genellikle uluslararası siber suç soruşturmalarına ciddi engeller oluşturmaktadır.

Uluslararası işbirliğinin önündeki engeller: uluslararası bağlamda, kanıtların süratle paylaşılması için ortak bir yasal çerçeve yoktur (kanıtların korunması için olduğu gibi). Sınır ötesi iletişim ve hızlı bilgi alışverişi için daha iyi bir mekanizmaya da ihtiyaç vardır.

Kamu-özel sektör ortaklıklarının zorlukları: siber suçla mücadelede özel sektörle işbirliği hayati önem taşımaktadır, ancak standartlaştırılmış katılım kuralları yoktur ve bu nedenle soruşturmalar engellenebilir." Bkz. EUROPOL, https://www.europol.europa.eu/newsroom/news/setting-scene-for-cybercrime-trends-and-new-challenges, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

tarafından siber suçlara ilişkin birçok operasyon da gerçekleştirilmekte[679] ve siber suçlarla mücadelede yakın işbirliği ve uzmanlık alışverişini kolaylaştırmak için işbirliği anlaşmaları da imzalamaktadır.[680]

Eurojust (European Agency for the Enhancement of Judicial Cooperation - Avrupa Adli İşbirliğinin Geliştirilmesi Ajansı) ise Avrupa Konseyi' nin 28.02.2002 tarihli ve 2002/187/JAI sayılı kararı ile ulusal yargı mercilerinin yetkinliğini artırmak ve sınır ötesi organize suçların soruşturulmasını yürütmek amacı ile kurulan ve üye ülkelerin hakim, savcı veya eşdeğer ayrıcalıklara haiz polis teşkilatı görevlilerinden oluşan bir teşkilattır.[681] Eurojust tarafından, 2016 yılında Avrupa Yargı Siber Suç Ağı (European Judicial Cybercrime Network - EJCN) başlatılmış olup bu proje ile siber suçların soruşturulması ve kovuşturulması ile ilgili uzmanlık, en iyi uygulama ve diğer ilgili bilgilerin değişimini sağlayarak yetkili adli makamlar arasındaki işbirliğini kolaylaştırma ve geliştirme bunun yanında siber alanda hukukun üstünlüğünü sağlamada rol oynayan farklı aktörler ve paydaşlar arasında diyalogu teşvik etme amacı gütmektedir.[682] Bunun yanında tüm bireylerin kişisel verilerini koruma, Eurojust' ın yasal çerçevesinin temel ilkelerinden biri olup Eurojust, veri koruma kurallarını ve süreçlerini güncelleme süreci içerisindedir.[683] Yine Eurojust tarafından, yakın bir zaman önce 5. Siber Suçlar Yargı Monitörü çalışması yayınlanmış olup monitör özellikle AB veri saklama kurallarının uygulanmasıyla ilgili en son veri saklama gelişmelerine genel bir bakış sunmakla beraber siber suç ve e-kanıt toplama

679 Bkz. EUROPOL, https://www.europol.europa.eu/newsroom/news/60-e-commerce-fraudsters-busted-during-international-operation, ET. 1 Mart 2020.

680 ENISA ve Europol arasında siber suçlarla mücadeleye ilişkin imzalanan işbirliği anlaşması için bkz. EUROPOL, https://www.europol.europa.eu/newsroom/news/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol, ET. 1 Mart 2020.

681 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 78, dipnot. 245.

682 EUROJUST, http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx, ET. 1 Mart 2020. Avrupa Yargı Siber Suç Ağı'nın (EJCN) yedinci genel toplantısı 14-15 Kasım 2019 tarihinde Eurojust' ta gerçekleştirilmiştir. Ayrıntılı bilgi için bkz. EUROJUST, http://www.eurojust.europa.eu/press/News/News/Pages/2019/2019-11-15_EJCN-7th-plenary.aspx, ET. 1 Mart 2020.

683 "Eurojust, veri koruma kurallarını ve süreçlerini güncelleme sürecindedir. Eurojust Tüzüğünün veri koruma hükümleri ve kişisel verilerin işlenmesine ilişkin güncellenmiş AB kuralları (Avrupa Parlamentosu ve Konsey'in 2018/1725 Tüzüğü) her ikisi de Aralık 2019'da yürürlüğe girmiştir ." bkz. EUROJUST, http://www.eurojust.europa.eu/Practitioners/Data-Protection/Pages/Data-protection-at-Eurojust.aspx, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

ile ilgili ulusal yasal gelişmeleri ve son dönüm noktası mahkeme kararlarını da incelemektedir.[684]

2.1.5. Avrupa Konseyi Çalışmaları ve Avrupa Konseyi Siber Suç Sözleşmesi (Sanal Ortamda İşlenen Suçlar Sözleşmesi)

2.1.5.1. Avrupa Konseyi Çalışmaları

Avrupa çapında insan hakları, demokrasi ve hukukun üstünlüğünü savunmak amacıyla 1949'da kurulmuş hükûmetlerarası bir kuruluş[685] olan Avrupa Konseyi (AK) ise 1973 ve 1974 yılında Bakanlar Komitesince elektronik veri bankalarında uygulanacak ilkeleri içeren iki öneri kararı kabul etmiş ve bazı ülkeler hukuk mevzuatlarını buna göre uyarlamış, elektronik veri bankalarında saklanan kişilerin özel hayatına ilişkin verileri koruma amacıyla 28 Ocak 1981 yılında "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması" na ilişkin 108 sayılı Sözleşme imzaya açılarak ülkemiz tarafından da söz konusu Sözleşme' yi imzalamıştır.[686] Bunun yanında Avrupa Konseyi OECD' nin 1986 yılında hazırlamış olduğu raporu esas alarak raporda belirlenmiş olan eylemlerin üye ülkeler nezdinde cezai yaptırım altına alınmasını bunun yanında rapora ek olarak bilgisayarla bağlantılı suçlarla ilgili korunma, engellenme, mağdurlar, uluslararası araştırmalar, veri bankalarına el konulması, bilgisayar suçlarının soruşturma ve kovuşturmasında uluslararası işbirliğine gidilmesi konularında taslak metin çalışması gerçekleştirmiş, bu metin ise Bakanlar Komitesi tarafından 13 Eylül 1989' da yürürlüğe girmiştir.[687] Yine Avrupa Konseyi Bakanlar Komitesi' nce 11 Eylül 1995 yılında, bilişim teknolojilerinin getirmiş olduğu yeniliklere uyacak şekilde ceza usul yasalarında yer alan soruşturma ve el koymaya ait hükümlerin revize edilmesi, elektronik delil, şifreleme sistemlerinin kullanılması, uluslararası işbirliği başlıkları altında ceza usul yasalarında gerçekleştirilecek değişikliklere ilişkin kuralları kabul etmiştir.[688]

---

684 Ayrıntılı bilgi için bkz. EUROJUST, http://www.eurojust.europa.eu/press/News/News/Pages/2020/2020-01-28_Cybercrime-Judicial-Monitor-Issue5.aspx, ET. 1 Mart 2020.

685 https://tr.wikipedia.org/wiki/Avrupa_Konseyi, ET. 29 Şubat 2020.

686 Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", s. 2752; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 197.

687 Eker, a.g.e., s. 110; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 197.

688 Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", s. 2753; Eker, a.g.e., s. 110; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 197.

Avrupa Konseyi tarafından bilişim suçları alanında en kapsamlı uluslararası belge olan Budapeşte Sözleşmesi veya Avrupa Konseyi Siber Suçlar Sözleşmesi, "Avrupa Konseyi Suç Sorunları Komitesi"[689] nin (Council of Europe European Committee on Crime Problems- CDPC) 1996 yılında CDPC/103/211196 sayılı kararı ile siber alanda işlenen suçlar üzerinde çalışmak üzere oluşturulan uzmanlar komitesinin[690] Siber Suçlar Sözleşme Taslağı ve açıklayıcı raporunu Haziran 2001' de Avrupa Konseyi Suç Sorunları Komitesi' ne sunması üzerine 8 Kasım 2001' de Avrupa Konseyi Bakanlar Komitesi' nce kabul edilerek 23 Kasım 2001' de Budapeşte' de düzenlenmiş olan Siber Suçlar Uluslararası Konferansında imzaya sunulmuş ve üç Avrupa Konseyi üyesi devletin onay belgelerini sunması ile 1 Haziran 2004' te yürürlüğe girmiştir.[691] Sözleşme, ülkemiz tarafından 10 Kasım 2010 tarihinde imzalanarak 22 Nisan 2014 tarihli ve 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile onaylanmıştır.[692]

689 Ayrıntılı bilgi için bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cdpc, ET. 29 Şubat 2020.

690 CDPC kararı gerekçesi ve komitenin görev tanımı hakkında ayrıntılı bilgi için bkz. Kayıhan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri" ", s. 4,5, https://docplayer.biz.tr/33880825-Avrupa-konseyi-siber-suc-sozlesmesi-baglaminda-avrupa-siber-suc-politikasinin-ana-ilkeleri.html, ET. 1 Mart 2020; Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s.13-15.

691 Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", s. 2753; Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 15.

692 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 21.

Türkiye' nin Sözleşmeye koyduğu çekinceler ise şunlardır:

"1) 40. madde ve 2. maddeye istinaden, Türkiye Cumhuriyeti Devleti, suçun bilgisayar verilerini elde etmek veya başka bir sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koştuğunu beyan eder.

2) 40. madde ve 7. maddeye istinaden, Türkiye Cumhuriyeti Devleti, bilgisayarla bağlantılı sahteciliğe ilişkin 7. maddedeki suç tanımının Türk kanunlarına göre dolandırma veya benzeri hileli davranış kastını gerektirdiğini beyan eder.

3) 42. madde ve 14. maddenin 3 (b) paragrafına istinaden, Türkiye Cumhuriyeti, herhangi bir hizmet sağlayıcının bilgisayar sistemi üzerinden iletişime ilişkin olarak, söz konusu sistemin belli bir kullanıcı grubunun menfaatine işletiliyor olması; halka açık iletişim şebekelerini kullanmıyor olması ve halka açık ya da özel nitelikli başka bir bilgisayar sistemine bağlı olmaması halinde, söz konusu aktarıma ilişkin olarak 20'nci ve 21'nci maddelerde belirtilen önlemleri uygulamama hakkını saklı tutar.

4) 42. madde ve 22. maddeye istinaden, Türkiye Cumhuriyeti Devleti, Türk vatandaşının yurt dışında işlemiş olduğu suçlardan dolayı Türk Ceza Kanununun 11. Ve 13. maddesi çerçevesinde yargı yetkisini kullanma hakkını saklı tutar.

5) 42. madde ve 29. maddenin 4. paragrafına istinaden, Türkiye Cumhuriyeti Devleti, çifte suçluluk şartının verilerin açıklandığı tarihte yerine getirilemiyor olduğuna ilişkin gerekçeler bulunması halinde, işbu madde çerçevesinde verilerin korunması talebini reddetme hakkını saklı tutar.

6) 24. maddenin 7 (a) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, suçluların iadesine ilişkin anlaşma mevcut olmadığı durumlarda, suçluların iadesi veya geçici tutuklama taleplerini iletmek veya almak üzere Adalet Bakanlığını yetkili makam olarak belirler.

Resmi tercümesi "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak belirtilen ve 10 Kasım 2010 tarihinde imzalanan sözleşme, 22 Nisan 2014 tarihli ve 6533 sayılı "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun" ile uygun bulunarak 2 Mayıs 2014 tarihli ve 28988 sayılı Resmi Gazete' de yayımlanarak yürürlüğe girmiştir.[693] Avrupa Konseyi Siber Suçlar Sözleşmesi[694] (AKSS), ulusal mevzuat geliştiren her ülke için bir rehber ve anlaşmaya taraf devletler arasında uluslararası işbirliği için bir çerçeve görevi görmekte olup bilgisayar sistemleri yoluyla yapılan Yabancı Düşmanlığı ve Irkçılık Protokolü ile de desteklenmektedir.[695] Üye Devletlerin ve diğer üye olmayan Devletlerin katılımına ve katılımına katılan üye olmayanların imzasına açık antlaşma olmasının yanında Sözleşme, özellikle telif hakkı, bilgisayarla ilgili dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlallerini ele alan, İnternet ve diğer bilgisayar ağları üzerinden işlenen suçlarla ilgili ilk uluslararası antlaşma özelliğini taşımakta, ayrıca, bilgisayar ağlarının aranması ve müdahale gibi bir dizi güç ve prosedür içermektedir.[696] Sözleşme' nin temel amacı, özellikle uygun mevzuatı kabul ederek ve uluslararası işbirliğini teşvik ederek toplumun siber suçlara karşı korunmasını amaçlayan ortak bir ceza politikası

7) 27. maddenin 2 (c) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, karşılıklı yardım taleplerinde bulunmak, talepleri yanıtlamak, bu taleplerin gereğini yerine getirmek veya bunların gereğini yerine getirecek makamlara bu talepleri iletmekle Adalet Bakanlığını merkezi makam olarak belirler.

8) 35. maddenin 1. Paragrafına istinaden, Türkiye Cumhuriyeti Devleti, 7 gün / 24 saat esasına göre temas noktasının Emniyet Genel Müdürlüğü Bilişim Suçlarıyla Mücadele Daire Başkanlığı olduğunu beyan eder." Bkz. A.e., s. 77.

693 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 236.

694 "23 Kasım'da Avrupa Konseyi, Siber Suç Konvansiyonu'nun 17. Yılını kutladı. Bu vesileyle, Avrupa Konseyi'ne Tarafların ve Gözlemcilerin Daimi Temsilleri, siber suçların mevcut zorlukları ve Avrupa Konseyi'nin yanıtı hakkında bilgilendirildi.

Toplantı Büyükelçi Corina Calugaru, Moldova Daimi Temsilcisi ve Bilgi Politikası Tematik Koordinatörü girişimi ile düzenlendi.

Katılımcılar, 2001 yılından bu yana, Budapeşte Konvansiyonunun küresel ölçekte Avrupa Konseyi'nin en etkili antlaşmalarından biri haline geldiğini, siber suç ve elektronik kanıtlar üzerine kapsamlı ve tutarlı bir çerçeve sağladığını kabul etti.

Sözleşme, siber suçlara karşı ulusal mevzuat geliştiren her ülke için bir rehber ve bu anlaşmaya Taraf Devletler arasında uluslararası işbirliği için bir çerçeve görevi görmektedir.

Siber Suçlar Konvansiyonu'nun şu anda 61 Taraf Devleti var. 10 Devlet daha imzaladı veya katılmaya davet edildi." Bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/17th-anniversary-of-the-budapest-convention, ET. 29 Şubat 2020. (Google translate ile çeviri yapılmıştır.)

695 COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/the-budapest-convention, ET. 29 Şubat 2020.

"Türkiye, 19 Nisan 2016'da bilgisayar sistemleri aracılığıyla işlenen ırkçı ve yabancı düşmanlığı niteliğindeki fiillerin kriminalize edilmesine ilişkin Siber Suç Sözleşmesi'ne Ek Protokolü imzalamıştır." Bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/turkey-signed-the-protocol-on-racism-and-xenophobia, ET. 29 Şubat 2020. (Google translate ile çeviri yapılmıştır.)

696 COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, ET. 29 Şubat 2020.

izlemektir.[697] Budapeşte Siber Suç Konvansiyonu tarafları, 8 Haziran 2017' de "Siber Suçlar Konvansiyon Komitesi (Cybercrime Convention Committee - T-CY)"[698] nin 17. Genel Kurulu' nda kolluk kuvvetlerinin yabancı, çoklu veya bilinmeyen yargı bölgelerindeki sunucular üzerinde kanıt sağlamasına yardımcı olmak için antlaşma için bir protokol hazırlanmasını kabul etmiş[699], 2000 yılından bu yana Kore Ulusal Polisi tarafından her yıl düzenlenen ve 29-31 Ağustos 2018' de Kore'nin Seul şehrinde gerçekleştirilen Uluslararası Siber Suç Tepkisi Sempozyumu' nda ise Budapeşte Sözleşmesine ek bir Protokol yönünde ilerleme konusu tartışılmıştır.[700]

Avrupa Konseyi Siber Suçlar Konvansiyon Komitesi tarafından, 27 ve 28 Kasım 2017' de Strazburg'da gerçekleştirilen 18. Genel Kurul toplantısında gelişmiş uluslararası işbirliği ve bulutta elektronik kanıtlara erişim konusunda Budapeşte Konvansiyonu için bir Ek Protokol müzakere edilmiş[701], aynı komite tarafından buluttaki verilere etkili ceza adaleti erişimi, daha etkili karşılıklı yasal yardım, verilerin kamusal/özel paylaşımı gibi konu başlıklarını içeren "Sınırları aşmak: siber alanda yargı yetkisi" konferansı, 7-8 Mart 2016 tarihlerinde Amsterdam'da gerçekleştirilmiştir.[702]

Avrupa Konseyi, Romanya' daki "Siber Suçlar Programı Ofisi (Cybercrime Programme Office - C-PROC)"[703] aracılığıyla da dünya çapında ülkeleri siber suçlar

---

697 A.e.

698 "Siber Suçlar Sözleşmesi Komitesi (T-CY), Budapeşte Siber Suçlar Sözleşmesi'nin Taraf Devletlerini temsil eder. Sözleşme'nin 46. maddesine dayanarak, Komite'nin istişaresi, Sözleşmenin etkili kullanımını ve uygulanmasını, bilgi alışverişini ve gelecekteki değişikliklerin dikkate alınmasını kolaylaştırmayı amaçlamaktadır." Bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/tcy, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)
Komite raporları için bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/t-cy-reports, ET. 29 Şubat 2020.

699 Ayrıntılı bilgi için bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud, ET. 29 Şubat 2020.

700 COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/the-budapest-convention-at-iscr-2018, ET. 29 Şubat 2020.
Siber Suç Sözleşmesi'ne (ETS 185) bir taslak İkinci Ek Protokolün hazırlanmasında T-CY Genel Kuruluna yardımcı olmak üzere taslak hazırlama grubu oluşturulmuş olup grubun toplantı ve müzakereleri devam etmektedir. Toplantı raporları ve çalışmanın aşamaları konusunda ayrıntılı bilgi için bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/t-cy-drafting-group, ET. 1 Mart 2020.

701 COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/effectiveness-of-the-mutual-legal-assistance-and-cyberviolence-in-the-focus-of-the-18th-plenary-of-the-t-cy, ET. 29 Şubat 2020.

702 COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/jurisdiction-in-cyberspace-amsterdam-conference-concludes, ET. 1 Mart 2020.

703 "C-PROC, kapasite geliştirme işlevi ile, Taraf Devletlerin Budapeşte Sözleşmesinin uygulanmasını takip ettikleri Siber Suçlar Konvansiyon Komitesi'nin (T-CY) çalışmalarını tamamlamaktadır ." Ayrıntılı bilgi için bkz. COUNCIL OF EUROPE,

ve elektronik kanıtlarla ilgili siber suçlar ve elektronik kanıtların ortaya koyduğu zorluklarla mücadelede ceza adalet kapasitelerinin güçlendirilmesinde destek ve kapasite geliştirme çalışmaları yürütmektedir, iPROCEEDS (2016-2019), PGG 2018: Siber Suçlar @ EAP (2018), CyberCrime @ EAP III (2015-2017), CyberCrime @ EAP II (2015-2017), GLACY (2013-2016), Global Proje Aşama III (2012-2013), Siber Suçlar @ EAP I (2011-2014), Siber Suçlar @ IPA (2010-2013), Global Proje Aşaması II (2009-2011), Gürcistan'da Siber Suç Projesi (2009-2010), Global Proje Aşama I (2006-2009) gibi tamamlanmış projelerinin yanında iPROCEEDS-2 (2020-2023), "CyberEast (2019-2022)"[704], EndOCSEA @ Europe (2018-2020), "CyberSouth (2017-2020)"[705], "GLACY + (2016-2021)"[706], " Cybercrime @ Octopus - Siber Suç @ Ahtapot (2014-2020)"[707] devam eden projeleri bulunmaktadır.[708] iPROCEEDS-2 (2020-2023) Projesi, proje ülkelerindeki ve alanlardaki yetkililerin siber suç gelirlerini arama, ele geçirme ve el koyma kapasitelerinin daha da güçlendirilmesi ve internette kara para aklamanın önlenmesi ve elektronik kanıtların güvence altına alınması amaçlarını gütmekte olan Katılım Öncesi Mali Yardım Aracı

https://www.coe.int/web/cybercrime/cybercrime-office-c-proc-, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

704 "Proje, Siber Suç ve ilgili araçlarla ilgili Budapeşte Sözleşmesine uygun yasal ve politika çerçevelerini benimsemeyi, yargı ve kolluk kuvvetleri ile kurumlar arası işbirliğinin kapasitelerini güçlendirmeyi ve ceza adaleti, siber suçlar ve elektronik kanıtlar üzerine servis sağlayıcılar ve kolluk kuvvetleri arasında etkili uluslararası işbirliğini ve güveni artırmayı amaçlamaktadır." Bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/cybereast, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

705 "Avrupa Birliği (Avrupa Komşuluk Aracı) ve Avrupa Konseyi'nin ortak bir projesidir . CyberSouth insan hakları ve hukukun üstünlüğü gereklilikleri doğrultusunda Güney Komşuluk bölgesinde siber suçlar ve elektronik kanıtlarla ilgili mevzuatı ve kurumsal kapasiteleri güçlendirmeyi amaçlamaktadır." Bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/cybersouth, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

706 "GLACY +, Avrupa Birliği (Barış ve İstikrara katkıda bulunan Araç) ve Avrupa Konseyi'nin ortak bir projesidir.

…Dünya çapında devletlerin siber suçlar ve elektronik kanıtlarla ilgili mevzuatı uygulama kapasitelerini güçlendirmek ve bu alanda etkili uluslararası işbirliği yeteneklerini geliştirmek.

1. Tutarlı siber suç mevzuatını, politikalarını ve stratejilerini teşvik etmek;
2. Polis yetkililerinin siber suçları araştırma ve birbirleriyle ve Avrupa ile diğer bölgelerdeki siber suç birimleriyle etkin bir polis-polis işbirliği yapma kapasitesini güçlendirmek;
3. Ceza adaleti makamlarının mevzuat uygulamalarını ve siber suç ve elektronik kanıt davalarını yargılamalarını ve yargılamalarını ve uluslararası işbirliğine girmelerini sağlamak." Bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/glacyplus, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

707 "Siber Suç @ Ahtapot, dünya çapında ülkelere Budapeşte Siber Suç Sözleşmesi'ni uygulamalarına yardımcı olmayı ve veri korumayı ve hukukun korunması kurallarını güçlendirmeyi amaçlayan gönüllü katkılara dayalı bir Avrupa Konseyi projesidir." Bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/cybercrime-octopus, ET. 1 Mart 2020. (Google translate ile çeviri yapılmıştır.)

708 Ayrıntılı bilgi için bkz. COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/capacity-building-programmes, ET. 29 Şubat 2020.

(IPA) kapsamında Siber Suçlar İşbirliği, Avrupa Birliği ve Avrupa Konseyi'nin ortak bir projesi olup Türkiye de projeye katılan ülkeler arasında yer almaktadır.[709] Yine Türkiye' nin de katılan ülkeler arasında yer aldığı EndOCSEA @ Europe (2018-2020) Projesi, çocuk cinsel sömürüsünü ve istismarını önlemek ve bunlarla mücadele etmek için etkili çok uluslu, disiplinler arası ve sektörler arası işbirliği ve çocuk dostu önlemler ile korunmasını sağlama amacı gütmekte olup Avrupa Konseyi Çocuk Hakları Stratejisi (2016-2021) çerçevesinde uygulanan bu proje, ilgili uluslararası ve Avrupa standartlarının özellikle de Çocukların Korunmasına İlişkin Avrupa Konseyi Sözleşmesi' nin uygulanmasını destekleyecektir.[710]

2.1.5.2. Avrupa Konseyi Siber Suç Sözleşmesi (Sanal Ortamda İşlenen Suçlar Sözleşmesi)

Sözleşmenin açıklayıcı raporunda belirtilen temel amaçları:

"1) Bilişim suçlarıyla ilgili taraf devletlerin yasal mevzuatlarını ve bağlantılı hükümlerini uyumlu hale getirmek,

2) Siber suçların ve elektronik delil içeren diğer klasik suçların soruşturma ve kovuşturulması ile ilgili ulusal usul hukuku mevzuatına temel oluşturarak uluslararası muhakeme kurallarının yeknesaklaştırılmasını sağlamak,

*3) Uluslararası adli yardım ve işbirliği alanında hızlı ve etkili bir sistem oluşturmak"*şeklinde belirtilmiştir.[711]

Başka bir anlatımla, Sözleşme' nin bazı suçların ortak tanımının yapılması suretiyle, ulusal düzeyde mevzuatın uyumlulaştırılmasını sağlamak[712], siber suçların soruşturulmasında bilişim ortamına uygun düşen ortak yetkileri tanımlayarak devletler arasındaki muhakeme kurallarının yeknesaklaştırılmasını sağlamak ve hem geleneksel

709 COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/iproceeds-2, ET. 1 Mart 2020.

710 COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/endocsea-europe, ET. 1 Mart 2020.

711 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* s. 25; Cahit Aliusta ve Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt:4, No:2, ss. 35-42, 2018, s. 38.

712 Nitekim, "…kanunlardaki yetersizlikler nedeniyle bir ülkede suç olarak kabul edilen bir fiilin, başka bir ülkede suç sayılmaması veya o ülkede söz konusu fiile ilişkin herhangi bir mevzuat bulunmaması, suçlular için "güvenli sığınaklar" oluşturmaktadır. Özellikle bilişim suçlarının sınır aşan nitelikleri ve etkili, hızlı bir adaletin sağlanması gereği ve ayrıca soruşturma makanlarınca uluslararası kanallara sorunsuz ve doğrudan ulaşılmasının zorunlulukları birlikte değerlendirildiğinde, tüm dünya devletlerinin bu Sözleşme'ye en kısa zamanda taraf olması ve uluslararası işbirliği alanında hızlı ve etkili bir sistem kurulması gerekmektedir." Bkz. Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 26.

hem de yeni türden uluslararası işbirliği yöntemlerini belirlenerek devletlerin bu hükümleri bir an önce uygulamasını mümkün kılmak gibi temel üç amacı bulunduğu[713] ve esasen ana hedefinin de öncelikle ortak bir ceza politikası oluşturmak olduğu söylenebilmektedir.[714]

Avrupa Siber Suçlar Sözleşmesi, 48 m. ve 4 ana bölümden oluşmakta olup birinci bölümde, sözleşmede kullanılan terimlerin tanımlarına yer verilen maddeler yer almakta, ikinci bölümde, ulusal düzeyde alınacak önlemlere yer verilmiş, ikinci bölüm de kendi içerisinde üç kısıma ayrılarak önce maddi ceza hukuku düzenlemeleri başka bir ifade ile suç olarak kabul edilecek eylemler, suç tipleri tanımlanarak ardından muhakeme hukuku kapsamında usuli düzenlemelere yer verilmiş ve sonrasındaki kısımda da yargı yetkisine ilişkin genel ilkeler belirlenmiştir.[715] Sözleşmenin en önemli olduğu belirtilen üçüncü bölümde ise uluslararası adli yardımlaşma düzenlenerek kendi içerisinde iki bölüme ayrılmış, birinci kısımda uluslararası işbirliği ve iadeye ilişkin hususlar, ikinci kısımda ise ikinci bölümde yer alan usul hukukuna ilişkin hükümlerin uluslararası işbirliği karşısındaki durumu ele alınarak 7 / 24 uluslararası işbirliğinin devamı için gerekli sistemin kurulması emredilmiştir.[716] Dördüncü bölümde ise Sözleşme'nin uygulanmasına dair Sözleşme' nin yürürlüğü, çekince imkanı, anlaşmazlıkların çözümü gibi birtakım usuli ve teknik hükümler yer almaktadır.[717]

Sözleşmenin ikinci bölümünün birinci kısmında "Maddî Ceza Hukuku" başlığı altında:

1- "Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine Karşı Suçlar" başlığı altında Bilgisayar veri veya sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar (m. 2: hukuka aykırı erişim, m. 3: hukuka aykırı müdahale, m. 4: verilere müdahale, m. 5: bilişim sistemine müdahale, m. 6: cihazların kötüye kullanımı),

2- " Bilgisayarlarla Bağlantılı Suçlar" başlığı altında (m. 7: bilgisayarla ilgili sahtecilik eylemleri, m. 8: bilgisayarla bağlantılı dolandırıcılık eylemleri),

713 Önok, a.g.e., s. 1242.
714 Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, s. 25
715 A.e., s. 32, 33; Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 49; Aliusta ve Benzer, a.g.e., s. 38.
716 A.e.
717 A.e.

3- “İçerikle İlgili Suçlar” başlığı altında (m. 9: çocuk pornografisi ile ilgili suçlar),

4- “Telif Haklarının ve Benzer Hakların İhlali İle İlgili Suçlar” başlığı altında (m. 10: Telif Hakları ve Benzer Hakların İhlali İle İlgili Suçlar) suç tipleri düzenlenmiştir.[718]

Sözleşme ikinci bölümde belirlenmiş olan suç tiplerini birebir iç hukuk düzenlemesi haline getirilmesini zorunlu tutmamakla beraber maddi ceza hukuku mevzuatların içerik anlamında sözleşme düzenlemeleriyle uyumlu olmasını yeterli saymaktadır.[719] Başka bir anlatımla, Sözleşme, bilişim suçları ile mücadelede hukuk ve uygulama birliği istemekle birlikte taraf devletlerin özel ihtiyaçları doğrultusunda kendilerinin belli standartlar koyabilecekleri ve bu şekilde sözleşmeye uyabilecekleri benimsenmekte ve sözleşme ile tam bir uyum beklenmemektedir.[720] Ancak, Sözleşme’ de yer alan tüm hükümlerini tercüme ederek tam bir model kabul etmek suretiyle iç hukuklarına dâhil eden Romanya ve Portekiz gibi ülkeler de mevcut bulunmaktadır.[721] Bunun yanında bilişim suçlarının Sözleşmede kullanılan terimi ile siber suçların üzerinde fikirbiliği bulunan bir tanımının bulunmayışı sözleşmede de siber suç tanımının bulunmayışına sebebiyet vermiş, siber suçların içerik ve kapsamına yönelik suç tipleri belirlenerek ülkelerin bu doğrultuda düzenlemeler yapmaları beklenmiştir.[722]

Sözleşmenin diğer bölümlerinde düzenlenmiş olan tanımlar, adli yardımlaşma, usul hükümleri vb. hükümler bilişim suçları ile mücadelede önemli düzenlemeler içermekte olup çalışma konumuzu mevcut TCK’ da “Bilişim Alanında Suçlar” başlığı altında düzenlenmiş olan bilişim suçları oluşturduğundan bu başlık içerisinde Sözleşme’ nin ikinci bölümünün birinci kısmında “Maddî Ceza Hukuku” başlığı altında düzenlenmiş olan suç tipleri üzerinde durulacak[723], diğer bölümlerde düzenlenen hükümlere ise yeri geldikçe ilgili başlıklar altında değinmekle yetinilecektir.

718 Değirmenci, “Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi”, s. 2754.
Düzenlenen suç tipleri hakkında ayrıntılı bilgi için bkz. Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları,* s. 50-53.
719 Aliusta ve Benzer, a.g.e., s. 38.
720 Akpek, a.g.e., s. 31, 56.
721 A.e., s. 31; Aliusta ve Benzer, a.g.e., s. 38.
722 Eryaman, a.g.e., s. 59.
723 “Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar” başlıklı 10. madde ise ulusal mevzuatımızda telif haklarının 5846 sayılı Fikri ve Sanat Eserleri Kanunu ile korunmuş ve bu Kanun kapsamında düzenlenmiş olması sebebiyle başlık içerisinde incelenmeyecektir.

"Yasadışı Erişim" başlıklı 2. m. :

"Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, sözkonusu suçun, bilgisayar verilerini elde etmek veya başka bir sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir."[724] hükmü düzenlenmiştir.

Bu suç ile korunmakta olan hukuksal yararın, bilgisayar sistemlerinin özgür ve serbest bir şekilde kullanımı ve yönetimi, başka bir deyişle bilgisayar sistemlerinin güvenliği olduğu belirtilmiştir.[725] Bir bilgisayar sistemi veya bir unsuruna kamusal telekomünikasyon ağları üzerinden veya bir kuruluşun yerel ağı (LAN) ya da Intranet' i gibi bir ağ üzerinden girmeyi içine alan "erişim" kavramı karşısında fazla sayıda e-posta gönderimi (spam) erişim tanımı kapsamında yer almamaktadır.[726] Nitekim, erişim kavramı ile o sistemin içine girmiş olunması gerekmemekte ddos ve spam e-posta gönderimi gibi bilişim suçlarını işleme yöntemlerinde sistemin içerisine girilmeden sisteme müdahale edilmektedir. "Yetkisiz erişim" hareketinin diğer suçların temelini oluşturabilecek nitelikte olması sebebiyle bu fiilin suç olarak düzenlenmesi önemli bir koruma sağlayabilecek niteliktedir.[727] Madde kapsamında başlı başına yetkisiz erişimin suç tipi olarak düzenlenmesi bazı taraf devletlerin suç ve ceza politikaları gereği ağır bir düzenleme niteliğinde olabileceğinden, maddenin devamında suçun daha nitelikli bir hale getirilebilmesi ihtimali düzenlenerek taraf devletlerin takdirine bırakılmıştır.[728] Sözleşmede düzenlenen yasadışı erişim ve araya

724 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, s. 14.

725 Akpek, a.g.e., s. 66.

726 Füsun Sokullu-Akıncı, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi", *İnternet Ortamında Ceza Sorumluluğu konulu panele sunulan bildiri*, s. 15, https://docplayer.biz.tr/24679386-Avrupa-konseyi-siber-suc-sozlesmesinde-yer-alan-maddi-ceza-hukukuna-iliskin-duzenlemeler-ve-ozellikle-internette-cocuk-pornografisi.html, ET. 3 Mart 2010; Nacar, a.g.e., s. 49.

727 Eryaman, a.g.e., s. 53.
"İzinsiz erişimi önlemenin en etkin yolu şüphesiz ki etkin güvenlik önlemlerinin geliştirilmesi ve uygulanmaya başlanmasıdır. Ancak kapsamlı bir önlem ceza hukukuna ilişkin yaptırımlarını kullanma tehdidini ve bu yaptırımların uygulamalarını da içermelidir. İzinsiz erişimin ceza yoluyla engellenmesi sistem ve veriler için ek bir koruma getirebilir ve yukarıda sayılan tehlikelerin erken bir aşamada önlenmesini sağlayabilir." Bkz. Sokullu-Akıncı, a.g.e., s. 15.

728 Akpek, a.g.e., s. 67.

girme suçları, bilişim sistemine yetkisiz giriş ve izleme, dinleme faaliyetlerini kapsamakta ve TCK' nın 243. m.' sine karşılık gelmektedir.[729]

"Yasadışı Müdahale" başlıklı 3. m. :

"Taraflardan her biri, bilgisayar verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dâhil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak gerçekleştirilen araya girme fiilinin, haksız yere ve kasten yapıldığı zaman, kendi iç hukuku kapsamında cezaî suç olarak tanımlaması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, sözkonusu suçun sahtekârlığa yönelik veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişkili olarak işlenmiş olmasını şart koşabilir."[730]

Sözkonusu maddede düzenlenen fiil veri iletimine "teknik yöntemler"[731] kullanılarak müdahale edilmesidir. Ayrıca madde kapsamında düzenlenen bir diğer husus ise kamuya açık olmayan bilgisayar verisi yayını olup verinin değil yayının özelliğini oluşturmaktadır.[732] Bu maddede korunan değerin ise, Avrupa İnsan Hakları Sözleşmesi' nin 8. m.' si ile teminat altına alınan kişilerin özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi ilkesinin bütün elektronik veri transferleri için uygulanmış hali başka bir deyişle haberleşmenin gizliliği hakkı ile aynı hak olduğu belirtilmektedir.[733]

Madde metninde düzenlenen "yasadışı araya girme" suçu ise 5237 sayılı TCK' nın ilk halinde yer almamasına karşın, 24.3.2016 tarihli ve 6698 sayılı Kanun' un 30. m.' si ile 5237 sayılı TCK' nın 243. m.' sine 4. fıkranın eklenmesi ile düzenlenmiştir.[734]

"Verilere Müdahale" başlıklı 4. m. :

729 Karagöz, a.g.e., s. 94.

730 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, s. 14.

731 "Teknik yöntemler, iletim hatlarına takılan teknik cihazları ve kablosuz iletişimi elde etmekte ve kaydetmekte kullanılan cihazları da kapsar. Bu yöntemler yazılım, şifre ve kodların kullanımını da kapsayabilir. Teknik yöntemler kullanma şartı, gereğinden fazla eylemi suç haline getirmemek için kullanılmış sınırlayıcı bir kavramdır." Bkz. Sokullu-Akıncı, a.g.e., s. 17.

732 Nacar, a.g.e., s. 50.
"İletilen veriler herkesin ulaşabileceği bilgiler olabilir, ama taraflar bunu gizlice iletmeyi isteyebilirler. Ya da ücretli televizyonlarda olduğu gibi, veriler hizmetin ücreti ödeninceye kadar ticari amaçlarla gizli tutulmak istenebilir. Bu nedenle, "kamuya açık olmayan" terimi tek başına kamusal ağlar üzerinden gerçekleştirilen iletişimleri dışarıda bırakmamaktadır." Bkz. Sokullu-Akıncı, a.g.e., s. 17.

733 Eryaman, a.g.e., s. 53; Akpek, a.g.e., s. 69.

734 Aliusta ve Benzer, a.g.e., s. 39.

"1 Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesini, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezaî 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."[735]

Madde içerisinde düzenlenen suç tipi ile geleneksel mala zarar verme suçuna benzer olarak bilgisayar veri ve programlarının da korunması amaçlanmış ve korunan hukuksal yarar olarak bilgisayar veri programlarının bütünlüğü ve düzgün bir şekilde işlemesi olarak görüldüğü belirtilmektedir.[736]

Sözleşme'nin 4. ve 5. m.' lerinde yer alan "verilere" ve "sisteme" müdahale suçları 5237 sayılı TCK' nın 244. m.' si ile karşılanmış olup AKSS ile yüksek oranda uyum içerisindedir.[737]

"Sisteme Müdahale" başlıklı 5. m. :

"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 cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir."[738]

Madde hükmü ile yaptırıma bağlanması istenen fiiller, sisteme veri yolu ile müdahale edilmesi veya sistemde mevcut verilere fiziki olmayan müdahalelerdir.[739] Madde kapsamında yapılan düzenlemenin amacının ise, bilgisayar verisi ve programlarının kullanımı, bütünlüğü ve sağlıklı işleyişine karşı zarar verme amacı güden fiillerin engellenmesi olduğu belirtilmektedir.[740] Madde düzenlemesine göre sisteme müdahale sonucu sistemin işleyişinin ciddi ölçüde aksaması gerekmekte olup hizmet aksatmaya yönelik olarak yapılan DoS saldırıları veya istek dışı sıklıkla ve çok fazla sayıda e-posta gönderilmesi (spam) suretiyle bilgisayar sisteminin tamamen veya kısmen engellenmesi halinde ciddi ölçüde bir aksamanın varlığı kabul

735 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, s. 14.

736 Sokullu-Akıncı, a.g.e., s. 72.

737 Aliusta ve Benzer, a.g.e., s. 39.

738 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, s. 15.

739 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları,* s. 50-53.

740 Nacar, a.g.e., s. 50.

edilebileceğinden maddede belirtilen suçun oluştuğu kabul edilebilecektir.[741] Ayrıca madde içerisinde açıkça siber terör düzenlenmemişse de maddede belirtilen fiillerin ülkelerin kritik alt yapı tesislerine yöneltmesi durumunda siber terörün de bu suç kapsamına gireceği belirtilmektedir.[742]

"Cihazların Kötüye Kullanımı" başlıklı 6. m. :

"1 Taraflardan her biri, kasten ve haksız yere gerçekleştirildiği zaman, aşağıdakilerin kendi iç hukuku kapsamında cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

a aşağıda belirtilenlerin 2 ila 5. maddelerde belirtilmiş herhangi bir suçun işlenmesi için kullanılmaları amacıyla üretimi, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı veya başka şekilde erişilebilir hale getirilmesi:

i bir bilgisayar programı da dâhil olmak üzere, öncelikli olarak yukarıda belirtilen 2 ila 5. maddelerde belirtilmiş herhangi bir suçu işlemek amacıyla tasarlanmış veya uyarlanmış bir cihaz;

ii bir bilgisayar sisteminin tamamına veya herhangi bir kısmına erişimi mümkün kılan bir bilgisayar şifresi, erişim kodu veya benzer bir veri.

ve

b yukarıda paragraf a.i veya ii' de atıfta bulunulmuş bir öğeye, 2 ila 5. maddelerde belirtilmiş herhangi bir suçun işlenmesi için kullanılması amacıyla bulundurma.

Taraflardan biri, yasa gereği cezaî sorumluluğun doğması için bahsi geçen öğelerden belli bir sayıda bulundurulmasını şart koşabilir.

2 İşbu madde, bu maddenin 1. Paragrafında atıfta bulunulan üretme, satma, kullanım amaçlı tedarik, ithalat, dağıtma veya başka şekilde erişilebilir hale getirme veya bulundurmanın, 2 ila 5. maddeler uyarınca suç işlemek maksadıyla gerçekleştirilmemesi durumunda, örneğin bir bilgisayar sisteminin yetkililerce test edilmesi veya korunmasının amaçlandığı hallerde, cezaî yükümlülük doğuracağı şeklinde yorumlanmayacaktır.

3 Taraflardan her biri, çekincenin işbu maddenin 1.a.ii paragrafında sözü edilen öğelerin satışı, dağıtımı veya başka şekilde erişilebilir hale getirilmesiyle alakalı

741 Akpek, a.g.e., s. 74.
"Sistemin işleyişini önleyen ya da önemli ölçüde yavaşlatan virüs gibi kötü amaçlı kodlar, ya da bir alıcıya sistemin iletişim işlevlerini engellemek üzere çok büyük miktarlarda elektronik posta gönderen programlar bu kapsamda düşünülebilir." Bkz. Sokullu-Akıncı, a.g.e., s. 20.
742 Eryaman, a.g.e., s. 55.
Ancak, Sözleşme' nin yeni nesil bilişim suçları olarak kabul edilen siber savaş ve siber terör konusunda yeteri kadar çözümü henüz sunmadığını belirten yazarlar da bulunmaktadır. Bkz. Yetim, a.g.e., s. 82.

olmaması kaydıyla, işbu maddenin 1.paragrafını uygulamama hakkını saklı tutabilir.''[743]

Madde metni ile bilgisayar korsanlarının suç işlemekte kullandıkları içerisinde virüs, Truva atı, ağ solucanları vb. kötü amaçlı yazılımların üretim, kullanım ve dağıtımını da suç haline getirdiği bunun yanında suçun oluşumu için failde suç işleme niyetini aradığı ancak, failde aranan bu niyetin varlığı ya da yokluğu ispatı, bilişim suçlarının yapısından kaynaklanan zorluklar (gerçek faile ve yeterli delile ulaşmada yaşanan güçlükler) nedeniyle, kolay olmayacağı da ifade edilebilecek başka bir hususu oluşturmaktadır.[744]

5237 sayılı TCK' nın ilk halinde "Bilgisayar veri veya sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar" bölümü içerisinde düzenlenen suç tipleri bakımından en önemli sayılabilecek eksikliği cihazların kötüye kullanımını suç sayan bir hükmün bulunmayışı idi ancak bilişim suçlarıyla etkin bir şekilde mücadele edilebilmesi ve AKKS' nin 6. m.' sine uyumlu bir düzenleme yapılabilmesi amacıyla 24.3.2016 tarihli ve 6698 sayılı Kanun' un 30. m.' si ile 5237 sayılı TCK' ya 245/A m.' si eklenmiş ve AKKS' nin 6. m.' si ile uyum sağlanmıştır.[745]

"Bilgisayarla Bağlantılı Sahtecilik" başlıklı 7. m. :

"Taraflardan her biri, özgün olmayan verilerle sonuçlanan yeni veri girme, verileri değiştirme, silme veya engelleme eylemlerinin, sözkonusu verilerin yasal açıdan özgün verilermiş gibi kabul edilmesi veya işlem görmesi niyetiyle, kasten ve haksız yere gerçekleştirildiği zaman, verilerin doğrudan okunabilir ve anlaşılabilir olup olmadığına bakılmaksızın, bu eylemlerin kendi iç hukukunda cezaî suç olarak tanımlaması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, cezaî yükümlülüğün doğması için, eylemin hile veya benzer bir sahtekârlık niyetiyle gerçekleştirilmiş olmasını şart koşabilir.''[746]

743 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, s. 15.

744 Eryaman, a.g.e., s. 55, 56.
Bilişim suçlarını işlemek için erişim araçlarının başka bir deyişle hacker araçlarının bulundurulması gerektiği, bu araçları suç işlemek için elde etmeye yönelik, üretim ve dağıtımları alanında bir tür karaborsanın doğabilme tehlikesi ile etkin bir biçimde mücadele edebilmek için, ceza hukuku tehlike potansiyeli taşıyan belirli fiillerin, Madde 2 – 5' te tanımlanan suçların işlenmesinden önce, kaynağında yasaklaması gerektiği belirtilmektedir. Bkz. Sokullu-Akıncı, a.g.e., s. 22, 23.

745 Aliusta ve Benzer, a.g.e., s. 39.

746 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, s. 16.

Madde metninde yapılan düzenleme ile korunan hukuksal değerin, elektronik verinin güvenliği ve güvenilirliği olduğu belirtilmektedir.[747] Madde metni ile bilgisayar verilerinin değiştirilmesi, silinmesi veya verilerin engellenmesi suretiyle sahte bir e-belgenin düzenlenmesi kast edilmekte[748] olup aldatmaya yönelik verilerin izinsiz olarak değiştirilmesi ya da yeni verilerin yaratılması, doğrudan orijinal verilerin hukuki anlamda delil özelliğinin değiştirilmesi ile ilgili olduğu belirtilmektedir.[749]

"Bilgisayarla Bağlantılı Dolandırıcılık" başlıklı 8. m. :

"Taraflardan her biri, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, bir başka şahsın mal kaybına sebebiyet verdiğinde, bunların kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

Şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekârlık niyetiyle;

a bilgisayar sistemlerine veri girişi yapma, verileri değiştirme, silme veya engelleme;

b bir bilgisayar sisteminin işleyişine herhangi bir müdahalede bulunma."[750]

Madde ile yaptırıma bağlanması istenilen, gerçeği yansıtmayan verinin sisteme eklenmesi yoluyla gerçekleştirilen değişiklikler veya veri işlenmesine yönelik müdahaleler yolu ile gerçekleştirilen yasaya aykırı mal transferleri olarak somutlaşmaktadır.[751] Madde düzenlemesi, TCK' nın 158. m.' sinin birinci fıkrasının b bendinde, dolandırıcılık suçunun işlenmesi halini suçun nitelikli hali olarak düzenlenerek karşılanmıştır.

"Çocuk Pornografisiyle Bağlantılı Suçlar" başlıklı 9. m. ise:

"1 Taraflardan her biri, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, bunların kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

a bir bilgisayar sistemi üzerinden dağıtımını yapmak amacıyla çocuk pornografisi üretmek;

b bir bilgisayar sistemi üzerinden çocuk pornografisini sunmak veya erişilebilir hale getirmek;

747 Nacar, a.g.e., s. 52.
748 Akpek, a.g.e., s. 79.
749 Eryaman, a.g.e., s. 56.
750 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, s. 16.
751 Nacar, a.g.e., s. 52.

c bir bilgisayar sistemi üzerinden çocuk pornografisinin dağıtım veya iletimini yapmak;

d kendisi veya başkası için bir bilgisayar sistemi üzerinden çocuk pornografisi temin etmek;

e bir bilgisayar sisteminde veya bilgisayar verileri depolama aygıtında çocuk pornografisi bulundurmak.

2 Yukarıda 1. Paragrafta belirtilen "çocuk pornografisi" terimi aşağıda belirtilenleri görsel anlamda tasvir eden pornografik malzemeleri içerecektir:

a reşit olmayan şahsın cinsel içerikli eylemlerde bulunması;

b reşit olmayan şahıs görüntüsüne haiz şahsın cinsel içerikli eylemlerde bulunması;

c reşit olmayan şahsın cinsel içerikli eylemlerde bulunmasını betimleyen gerçekçi görüntüler.

3 Yukarıda 2. Paragrafta belirtilen "reşit olmayan" terimi, 18 yaşın altındaki tüm şahısları kapsar. Bununla birlikte, Taraflardan biri, 16'dan küçük olmamak kaydıyla, daha düşük bir yaş sınırı talep edebilir.

4 Taraflardan her biri, 1. Paragrafın d ve e bentleri ile 2. Paragrafın b ve c bentlerinin tamamını veya bir kısmını uygulamaya koymama hakkını saklı tutabilirler."[752]

Madde metni ile yaptırıma bağlanması istenen suç tipi, TCK' nın yedinci bölüm genel ahlaka aykırı suçlar başlığı altında 226. m.' sinde yer alan müstehcenlik suçuna karşılık gelmekte olup çocuk pornografisinin özellikle Sözleşme'nin ilgili maddeleri örnek alınarak ayrı bir suç tipi olarak düzenlenmeyişinin Türk Ceza Hukuku açısından önemli bir eksiklik oluşturduğu belirtilmektedir.[753] Maddenin 3. fıkrasında kullanılan ifade çocuk pornografisi üretenleri içine almakla birlikte "basın ve yayın yolu ile yayınlayan", "yayınlanmasına aracılık eden", "başkalarının kullanımına sunan" gibi ifadeler de çocuk pornografisinin herhangi bir şekilde dağıtımını yasaklamakta[754] ise de TCK' nın 226. m.' sinde, içeriğin yalnızca basın ve yayın yolu ile yayılmasının düzenlenmiş olup açıkça bilişim sistemleri ifadesinin kullanılmamış olunması da bir eksiklik olarak değerlendirilmektedir.[755] Biz de bu görüşe katılmaktayız. Milliyet, cinsiyet ve yaş farkı gözetmeksizin dünyanın her yerinde çocukları ve çocuk haklarını ciddi anlamda tehdit eden, çocukların cinsel şiddete

752 TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, s. 16, 17.

753 Aliusta ve Benzer, a.g.e., s. 39.

754 Ahu Sinem Civiloğlu ve Güzin Tanyeri, "Bilişim Suçları ve Çocuk Pornografisi", *Hukuk Gündemi Dergisi*, Sayı: 7, Bahar 2007, ss. 95-101, s. 101.

755 Karagöz, a.g.e., s. 109.

maruz kalmasına ve bir ticari meta haline gelmesine sebebiyet veren bunun yanında günümüzde ve gelecekte de devletler için önemli bir sorun oluşturan çocuk pornografisi ile etkin mücadelede de diğer bilişim suçlarında olduğu gibi uluslararası işbirliği, ortak stratejilerin belirlenmesi ve tüm ülkelerin üzerinde anlaşabileceği gerçekçi ve uygulanabilir bir düzenlemenin yapılması şarttır.[756] Nitekim, bilişim teknolojilerinin geldiği nokta da düşünüldüğünde, bilişim sistemlerinin hayatımızın her alanına dahil olan "bilişim sistemleri kullanımının" TCK' nın 226. m.' si içerisine eklenmesi ve böylelikle güne uygun şekilde güncellenmesi gerektiği açıktır.[757]

2.2. BİLİŞİM SUÇLARINA İLİŞKİN YABANCI ULUSAL MEVZUATLARDA YER ALAN DÜZENLEMELER

Bilişim suçlarına ilişkin ülke düzenlemelerine bakıldığında, iki temel sistemin var olduğu söylenebilmektedir. Birinci sistem, bilişim suçlarına ilişkin suç ve cezai yaptırımların düzenlendiği hükümlerin ayrı bir kanun ile düzenlenmesi olup buna örnek olarak ABD' nin 1986 tarihli Bilgisayar Sahtekarlığı ve Bilgisayarın Kötüye Kullanılması Yasası, Avusturya' nın 1993 tarihli Otomatik Bilgi İşlem Suçları Yasası, İsrail' in 1997 tarihli Bilgisayar Suçları Yasası örnek olarak verilebilir.[758] İkinci sistem ise, bilişim suçları ile mücadelede (önlem ve yaptırım) ayrı bir kanunun düzenlenmeyip mevcut ceza kanunlarında bir takım değişiklikler gerçekleştirmektir.[759] Bu düzenlemelerde ise temelde üç farklı yöntem bulunduğu söylenebilmektedir. Birincisi, ceza kanunlarında bilişim suçlarına ilişkin özel hükümlerin eklenmesi (örneğin, Fransa, İtalya), ikincisi, halihazırda mevcut klasik anlamdaki suç tiplerinin yeniden tanımlanması, genişletilmesi veya yeni fiillerin eklenmesi (örneğin, Yunanistan, Kanada), üçüncüsü ise, 5237 sayılı TCK' nın da benimsemiş olduğu karma sistem olarak ifade edilen hem ayrı özel hükümlerin ihdası

756 A.e., s. 101.

757 Kara, Kaya' ya göre ise: "Son yıllarda Türkiye'de çocuk istismarına olan ilgi ve farkındalık yeterli olmamakla birlikte artmaktadır. Çocuk istismarı ile mücadelede yasal düzenlemeler mevcut haliyle yeni oluşan suç türleri için mücadelede yetersiz kalmaktadır. TCK Madde 103'te fiziki temas aranmaktadır. Ancak uygulamada ise çocukların online cinsel istismar suçunun TCK Madde 105 veya TCK. Madde 226-3 kapsamında değerlendirilmesi ile karşılaşılmaktadır. Çocukların online cinsel istismarı bilişim alanındaki suçlar kategorisinde sayılmamıştır. Ancak bilişim sistemleri aracılığıyla işlenen online çocuk cinsel istismar suçunun da bu başlık altında değerlendirilmesi gerektiği kanaatindeyiz." Bkz. Kara ve Kaya, a.g.e., s. 161.

758 Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", s. 2754, 2755.

759 A.e., s, 2755.

hem de klasik (geleneksel) anlamdaki suçların yeniden düzenlenmesi yolu ile genişletilmesidir.[760]

2.2.1. Amerika Birleşik Devletleri (ABD)

İnternetin doğum yeri olan ABD, internet kullanımının ortaya çıkardığı hukuki sorunlara ilişkin ilk hukuki düzenlemelerin getirildiği[761] ve federal ve eyaletler düzeyinde "sisteme yetkisiz giriş"e cezai işlem uygulayan ilk ülke[762] özelliği taşımaktadır. Günümüzde Microsoft, Apple, IBM, Google, Yahoo, Amazon gibi bilişim şirketleri ABD meşeili olduğundan ABD' de ekonomik istikrarın korunması adına bu şirketlerin üzerine oturduğu bilişim sistemlerinin ve esasen de internetin güvenli bir ortamda kullanımı şartlarının sağlanması gerekmekte, bu bağlamda bilişim sistemlerinin teknik güvenliğinin sağlanmasının yanında bilişim suçları ile etkin ve geniş çapta mücadelenin varlığı da zorunluluk oluşturmaktadır.[763] ABD' de federal düzeyde ve eyalet düzeyinde bilişim suçları konusunda, uluslararası kuruluşların düzenlemelerine de öncülük eden birçok düzenleme yapılmış[764] olup aşağıda federal kanunlardan bazıları örnek olarak incelenecektir.

1984 tarihli "Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Yasası"[765] (Computer Fraud and Abuse Act - CFFA) (federal yasa), Amerikan Temel Kanunu' nun 18. Bölümünün 1030. m.' sinin değiştirilmesi suretiyle gerçekleştirilmiş,[766] başlangıçta kısa ve dar ölçekli olması amaçlanan Kanun, günden

760 Eker, a.g.e., s. 108.

761 "Arizona, Florida, Illinois, Michigan, New Mexico, North Carolina, Rhode Island, California ve Virginia eyaletlerinde 70'li yıllarda bilişim suçlarına ilişkin özel düzenleme yapılmıştır." Bkz. Pallı, a.g.e., s. 93.

762 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 54.

763 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 212.

764 A.e., s. 213.

765 "1984 tarihli Bilgisayar Sahtekârlığı ve Bilgisayarların Kötüye Kullanılması Kanunu üç tip suç öngörmektedir. Birincisi, atom enerjisi, savunma veya dış başka bir ülke yararına kullanmak amacıyla yetkisiz olarak bilgisayarlara girme eylemi, ikincisi, finansal bilgiler elde etmek amacıyla gayrı meşru surette bilgisayarlara girilmesi veya bunların kullanılması, üçüncüsü, hükümet tarafından kullanılan bilgisayarlardaki bilgilerin tahribi, değiştirilmesi veya yok edilmesi fiilleridir. Ayrıca Federal Temel Kanunda bilgisayarlar kullanılarak müstehcen nitelikte materyaller oluşturulması bunların eyaletler veya dış ticaret yoluyla nakledilmesi, küçüğün rızaen veya kandırılarak, cinsel içerikli bir görsel materyalde oynatılması ve bu materyalin nakledilmesi, küçüğe ait görüntülerin daha sonradan seksüel içerikli kullanılacağını bile bile nakledilmesi, çocuk pornografisi de suç olarak düzenlenmiştir." Bkz. Kurt, a.g.e., s. 100.

766 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 213.

"1030. madde aşağıdaki davranışların herhangi birinin yapılmasını suç saymıştır. Bunlar:

- Bilerek yetkisizce veya verilen izni asarak bir bilgisayara erişmek ve böylece ya herhangi bir yabancı devletin yararına veya ABD'nin zararına kullanılabileceğine inanmak için failin haklı sebebinin bulunduğu, ifşa edilmemesi için korunan bir bilginin elde edilmesi ya da bir bilgiyi alma

güne artan ve bilgisayar güvenliğini tehdit eden eylemler sonucunda, Kongre tarafından 1988, 1989, 1990 ve 1994 yıllarında 4 kez değişikliğe uğramıştır.[767] Yedi bölüm içerisinde ulusal güvenlik bilgilerinin edinilmesi, bilişim sistemlerine erişim ve bilgi elde edilmesi, kamuya ait bilişim sistemlerine yetkisiz erişim, şifre kaçakçılığı, kasten veya taksirle bilişim sistemlerine yetkisiz giriş ve zarar verme eylemlerinin yaptırım altına alındığı suç tiplerinde 1 ila 20 yıl arasında hapis cezaları öngörülmüştür.[768] Kanun federal veya korunan bir bilgisayarı hedefleyen davranışları kapsamakta[769] başka bir deyişle kanunda koruma altındaki bir bilgisayara hukuka aykırı erişim ve bilgisayar verilerinin tahrip edilmesi ve değiştirilmesi fiilleri suç haline getirilmektedir.[770] Bilgisayarın bütünlüğüne yönelik suçları düzenleyen bu Kanunda öncelikle hükümet tarafından kullanılan sınıflandırılmış veya sınıflandırılmamış bilgiler korunmakta ise de Kanun geniş bir kapsamda özel ve kamusal bilişim sistemlerini korumak için düzenlenmiştir.[771] Kanunda yer verilen "koruma altındaki bilgisayar (protected computer)" ise "finansal bir kurum ya da devlet kurumlarına münhasıran kullanılan veya bunlarca dolaylı olarak kullanılıp suç fiilinin bunları etkilediği veya ABD dışında da olsa eyaletler arası ya da uluslararası ticaret veya iletişim maksadıyla kullanılan bilgisayardır."[772] 1984 ve 1986 tarihli

hakkı bulunmayan bir kişiye teslim etmek veya bilgiyi elinde tutmak ve teslim alma yetkisi bulunan bir federal ajana vermeyi reddetmek;

- Kasten yetkisizce veya verilen izni asarak bir bilgisayara erişmek ve böylece ya bir finans kurumunun mali kayıtlarını içeren bilgiyi veya bir kart dağıtıcısının veya müşteri rapor ajansının dosyasını içeren bilgiyi elde etmek ya herhangi bir federal bölüm veya ajanstan ya da eyaletler arası veya dış iletişimi içererek faaliyet gösteren korunan bir bilgisayardan bilgiyi almak; Ya sadece bir federal bölüm veya ajans tarafından kullanılan bir bilgisayara ya da faaliyeti federal hükûmet için veya federal hükûmet tarafından kullanılan bilgisayarları etkilediğinde sadece bir federal bölüm veya ajans tarafından kullanılmayan bir bilgisayara yetkisiz ve kasten erişim;
- Bilerek ve aldatmak niyetiyle yetkisiz veya yetki asılarak korunan bir bilgisayara erişmek ve böylece planlanan dolandırıcılığı ilerletmek ve dolandırıcılık nesnesi dışında yıllık 5000 doları geçmeyecek ve yalnızca bilgisayarın kullanımından oluşan herhangi bir değer elde etmek; Ya iletim, program, bilgi, kod veya komut nedeniyle korunan bir bilgisayara kasten zarar verme ya da korunan bir bilgisayara kasten ve yetkisizce erişip dikkatsizlikle zarara sebep olmak ya da korunan bir bilgisayara kasten ve yetkisizce erişmek ve böylece zarara sebep olmak;
- Federal hükûmet için veya federal hükûmet tarafından erişim hakkı elde edilebilecek bir bilgisayara girişte kullanılan şifre veya diğer bir bilginin dolandırıcılık niyetiyle ve bilerek eyaletler arası veya dış ticari etkileri bulunur şekilde ticaretini yapmak;
- Herhangi bir kişi, firma, dernek, eğitim kurumu, finans kurumu, hükûmet veya diğer yasal bir varlıktan zorla para veya değerli herhangi bir şey almak niyetiyle korunan bir bilgisayara zarar vermek için eyaletler arası veya dış ticaret alanında bir tehdit iletmek." Bkz. Pallı, a.g.e., s. 95, 96.

767 A.e., s. 95.

768 Karagöz, a.g.e., s. 95, 96.

769 Pallı, a.g.e., s. 94.

770 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 213.

771 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 173.

772 Eryaman, a.g.e., s. 42.

"Yorum farklılığına sebebiyet vermemek maksadıyla bilgisayar, finansal kurum, zarar, kayıp

Kanunlar ile devletin önemli ve gizli bilgilerinin saklandığı veya ülkenin kritik öneme haiz alt yapılarını işleten bilişim sistemlerinin korunmaya çalışıldığı, bu sistemlere yönelik eylemlerin ise siber suçlardan ziyade siber terör eylemleri ile örtüşmesi nedeniyle anılan yasaların da aslında siber terör tehlikesine karşı yürürlüğe konulmuş oldukları da ifade edilmektedir.[773] Bunun yanında ABD Federal Kanunu' na göre tüm kategorilerdeki bilgisayar suçlarını kapsayacak şekilde "erişim araçlarının" dolandırıcılıkta kullanılması hali suç olarak oluşturulmuştur.[774]

1986 tarihli Elektronik Haberleşme Gizliliği Kanunu' nda, bankamatik kartlarının meşru olmayan kullanımı, sahtesinin yapımı, sahte, tahrif edilmiş veya hukuk dışı yollardan elde edilmiş ya da diğer eyaletler veya dış memleketlerde çalınmış bir kartın kullanımı gibi eylemleri suç olarak düzenlemenin yanında bilgisayarlara meşru olmayan usullerle girilmesi suretiyle kullanılmasına ilişkin eylemleri suç haline getirmektedir.[775]

Bir diğer federal kanun 1996 yılında yürürlüğe giren ve çocuklar için zararlı içeriğe ulaşmalarının önlenmesi amacı güderek internet üzerinden yapılan yayınlara sınırlamalar getiren İletişim Ahlak Yasası, bu tür yayınları yapanlara hapis cezası ve para cezası yaptırımını kabul etmiştir.[776]

Yine 1996 yılında yürürlüğe giren "Çocuk Pornografisinin Önlenmesi Kanunu"[777] ve 1998 yılında yürürlüğe giren "Çocukların Online Yayınlardan Korunması Kanunu"[778] bulunmaktadır.[779] İletişimi durdurma, izleme ve dinleme gibi fiillerin cezalandırıldığı Telefon Dinleme Yasası'nda (Wiretap Act – 18/2511) 1986

---

gibi pek çok temel kavramın tanımlarına yer verilmiştir." Bkz. A.e.

773 A.e.

774 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 455.

"para, mal, hizmet veya değeri olan herhangi bir şeyi sağlamak için veya para fonlarının aktarımında kullanmak için (yalnızca kâğıt belge ile yapılan aktarımlardan farklı olarak); birlikte ya da tek başına erişim sağlayan; herhangi bir kart, plaka, kod, hesap numarası, elektronik seri numarası, mobil araç tanımlama numarası veya diğer telekomünikasyon hizmeti, donanımı veya tanımlayıcı aleti veya hesaba erişimde kullanılabilecek diğer araçlar" şeklinde tanımlanmıştır. Bkz. A.e.

775 Eryaman, a.g.e., s. 43.

776 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 213.

777 Bu Kanun ile Amerikan Temel Kanunu' nun 18. Bölümünün 2256. maddesinde gerekli değişiklikler yapılarak çocukların görüntülendiği pornografik yayın ve materyallerin elde bulundurulması, internet üzerinden ticaretinin yapılması veya internette yayınlanması yasaklanmaktadır. Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 57, dipnot. 250; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 214.

778 Kanun, normalde erişkinlerin erişimine açık olan pornografik sitelere çocukların erişiminin kolaylaştırılmasını suç olarak düzenlemekte ve hapis cezası ile para cezasını birlikte yaptırım altına almaktadır. Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 215.

779 A.e., s. 214, 215.

yılında gerçekleştirilen değişiklikte tüm elektronik iletişim ağları da suç kapsamında sayılmıştır.[780]

Belli eyaletler dışında yasaklanmış olan şans ve kumar oyunlarının internet yolu ile erişilebilir kılınmasını engelleme amacı güden 1997 yılında yürürlüğe giren "İnternet'te Kumarın Önlenmesi Yasası", kimlik bilgilerine hukuka aykırı olarak ulaşılması, bu bilgilerin hukuka aykırı amaçlar için kullanılması ve kullandırılması ve bilişim alanında her türlü sahtekarlık eylemin suç olarak düzenlendiği Amerikan Temel Kanunu' nun 1028. m.' de 1998 yılında gerçekleştirilen değişiklik ve bazı güvenlik hizmeti veren kamu kurumlarının bilişim sistemlerine hukuka aykırı erişimler ve bu sistemlerde bulunan verilere yönelik saldırıların "sanal terörizm suçu" adı altında düzenlendiği 2001 yılında yürürlüğe giren yeni Terörizmle Mücadele Kanunu bulunmaktadır.[781]

Son olarak belirtmek gerekir ki, ABD Avrupa Konseyi üyesi olmamakla birlikte AKSS' yi imzalayarak usulüne uygun olarak onaylamıştır.[782]

2.2.2. Fransa

Bilişim suçlarına ilişkin olarak Fransız Kanunu' nda ilk müstakil düzenleme 5 Ocak 1988 tarihinde yapılarak "hukuk dışı bir bilgisayara girilmesi veya sistemde hukuk dışı kalınması", "sistemdeki verilerin tahribi, değiştirilmesi veya yok edilmesi yahut başka veriler yüklenmesi", "sistemin işleyişinin engellenmesi veya bozulması", "bilgisayar belgelerinde sahtekârlık yapılması" ve "bu tür bir belgenin bilerek kullanımı" olarak beş adet bilişim suçu düzenlenmiştir.[783]

Fransa'da 01.03.1993 tarihinde yürürlüğe giren yeni Ceza Kanunu' nda ise "mala karşı diğer tecavüzler" başlıklı 11. Babın "verileri otomatik işleme tâbi tutmuş sistemlere yönelik saldırılar" başlıklı 111. Faslı içerisinde bilgisayar suçları düzenlenerek esasen eski kanuni düzenlemeden farklı bir düzenlemeye gidilmemiştir.[784] Yeni Fransız Kanunu' nda ayrıca kişilik haklarının bilişim sistemi aracılığıyla ihlali, otomatik sisteme bağlı kişisel verilerin ihlali, kişilerin resim ve

780 Karagöz, a.g.e., s. 96.
781 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 215.
782 A.e., s. 212.
783 Kurt, a.g.e., s. 103.
784 A.e.
"Tüm bilişim suçlarının tek bir fasıl içerisinde düzenlenmesi, suçların her birinin farklı hukuki yararı korumaları sebebiyle tüm faslı ilgilendiren genel hükümler de konulamadığından çok sık tekrarların yapılmasına sebebiyet vermiştir." Bkz. a.e.

sözlerinin kişinin rızasına aykırı biçimde montajının yayınlanması, "küçüğün fotoğrafının pornografik nitelikte kullanılması"[785], küçük tarafından görülmeye elverişli şiddet ve pornografik nitelikli mesaj yayımı, "bilişim sistemine tamamen veya kısmen haksız biçimde girme (bunun sonucunda girilen sisteme kaydedilmiş verileri silme, değiştirme veya sistemin fonksiyonlarını değiştirme filleri ağırlaştırıcı neden)"[786], "bilişim sisteminin işletiminin engellenmesi ya da tahrif edilmesi"[787] ve "bilişim sistemleri aracılığı ile dolandırıcılık"[788] fiilleri suç olarak düzenlemiştir.[789]

Fransa' da internetin düzenlenmesine ilişkin olarak ise 30.09.1986 tarihli ve 86-1067 sayılı Kanun' da 01.08.2000 tarih ve 2000-179 sayılı kanunla "Link üzerinde özel haberleşme dışındaki iletişim servisleriyle ilgili hükümler" eklenerek internet süjelerinin ceza sorumluluğu açısından bir ceza sistemi düzenlenmiştir.[790]

Fransız Ceza Kanunu'nda da "Bilgileri Otomatik Olarak İşleyen Sistemlere Yetkisiz Giriş" bölüm başlığı ile gibi salt bilişim suçlarına ayrı bir bölüm verilmiş fakat bölüm içerisinde yalnızca giriş değil, sistem içerisindeki verilere zarar verme fiili de cezalandırılmaktadır.[791] 765 Sayılı TCK'nın 2'nci Kitap 11'inci Bab'ında "Bilişim Alanında Suçlar" başlığı altında yer alan 525'inci m. Fransız sistemi esas alınmak

785 "Çocuğun pornografik içeriğe sahip bir fotoğrafı veya benzer bir temsilini edinen, kay-deden yayımlayan, ithal veya ihraç eden kişi 3 yıla kadar hapis ve 45.000 € para cezası ile cezalandırılır. Eylemin iletişim altyapısı kullanılarak herkesçe erişime açık hale getirilmesi halinde 5 yıla kadar hapis ve 75.000 € para cezası verilir. Suça teşebbüs de aynı cezaya tabiidir. (m. 227/23)" bkz. Karagöz, a.g.e., s. 99, 100.

786 "1- Bilgileri Otomatik İşleme Tabi Tutmuş Bir Sistemin Tamamına veya Bir Kısmına Aldatıcı Hareketlerle Erişmek (Girmek) Veya Kalmaya Devam Etmek (m. 323-1)
Bir sisteme hukuka aykırı olarak yetkisi olmadan girmesi ve hakkı olmadan kalınması suç haline getirilmiş, yapılan eylemler sistemdeki verilerin zarar görmesine, değişmesine, bozulmasına sebep olursa ceza artmaktadır" bkz. Nacar, a.g.e., s. 18.

787 "2- Bilgileri Otomatik İşleme Tabi Tutmuş Bir Sistemin Fonksiyonunu Bozucu veya Engelleyici Hareketlerde Bulunmak (m. 323-2)
Bilişim sistemleri kullanılarak işlenen suçlara Nas-ı Izrar Eylemleri de denir. 323-2 Maddesinde, bilgileri otomatik işleme tabi tutmuş bir sistemin fonksiyonunu bozucu veya engelleyici hareketlerde bulunmak, üç yıla kadar hapis ve 300.000 Franka kadar para cezasıyla cezalandırılmaktadır." Bkz. a.e., s. 21, 22.
"Bilişim sistemi içerisindeki verileri değiştiren, silen veya sahte gösteren kişi 5 yıla ka-dar hapis ve 75.000 € para cezası ile cezalandırılır. İlk üç maddedeki eylemleri gerçekleştirmek amacıyla bilgisayar programı veya cihaz ithal eden, üreten, bulunduran veya teklif eden kişi en ağır ceza ile cezalandırılır. (m. 323/3)" bkz. Karagöz, a.g.e., s. 99.

788 "5- Bilişim sistemleri Kullanılarak İşlenen Dolandırıcılık ve Sahtecilik Eylemleri;
Fransız Ceza Kanunu (md 147) özel hükümler içinde dolandırıcılık suçunun elektronik ortamda işlenmesini düzenlemektedir. 441-1'deki maddelerde de düzenlenen sahtecilik suçuna ilişkin hükümler artık bilişim alanındaki sahtecilik eylemlerini de kapsamaktadır. Bu suçlara teşebbüs ve iştirak 88-19. maddelerle cezalandırılmıştır." Bkz. Nacar, a.g.e., s. 23.

789 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 221, 222; Nacar, a.g.e., s. 18.

790 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 222; Nacar, a.g.e., s. 23.

791 Karagöz, a.g.e., s. 100.

suretiyle hazırlanmış ve Yargıtay uygulamaları ise bugüne değin sözkonusu kanuna göre şekillenmiştir.[792]

2.2.3. Almanya

Kıta Avrupa'sında bilişim suçları alanında ilk çalışma ve düzenlemelerin yapıldığı Almanya'da, bilişim suçlarına ilişkin maddi ceza hükümleri esas olarak Alman Ceza Kanunu içerisinde ve suçla korunan hukuksal değeri dikkate alınarak ilgili oldukları bölümde düzenlenmiştir.[793] Başka bir deyişle, Alman Ceza Kanunu, bilişim alanında suçları TCK' nın sistematiğinde olduğu gibi ayrı bir başlık altında ve müstakil bir bölümde ele almak yerine, Kanun'un değişik yerlerinde muhtelif hükümler içerisinde düzenlemiştir.[794]

"Verilere yetkisiz olarak (ulaşım) erişim imkanı sağlama" suçu:

> *"Madde 202a- (1) Yetkisiz olarak, kendisine ait olmayan ve haksız erişimlere karşı özel olarak güvenlik altına alınmış bulunan verilere, giriş güvenliğini kırarak kendisi veya bir başkası için erişme imkanı sağlayan kişi, üç yıla kadar hapis veya (adli) para cezası ile cezalandırılır.*
>
> *(2) Birinci fıkra anlamındaki veriler, sadece elektronik veya manyetik olarak ya da doğrudan algılanabilir olmayan başkaca herhangi bir şekilde saklanmış veya iletilen verilerdir."*[795]

"(Bilgisayar ağlarındaki) verileri yetkisiz olarak yakalama (ele geçirme)" suçu:

> *"Madde 202b- Teknik araçlar kullanarak, kamusal olmayan veri iletişimlerinden veya bir bilgi işlem sisteminin elektromanyetik dalgalarından yetkisiz olarak kendisi ya da bir başkası için verileri (m. 202a/2) yakalayan (ele geçiren) kişi, fiil başka hükümlerle daha ağır cezaya bağlanmamışsa, iki yıla kadar hapis veya (adli) para cezası ile cezalandırılır."* şeklinde düzenlenmiştir.

5237 sayılı TCK' nın 244. m.' sine yakın düzenleme niteliğindeki mala zarar verme (m. 303) kapsamında yaptırıma bağlanmış bulunan[796] "Verilerin değiştirilmesi":

---

792 Eryaman, a.g.e., s. 45.
793 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 219; Karagöz, a.g.e., s. 96.
794 Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: XIV, Sayı: 2, Yıl: 2010, ss. 275-303, s. 285, http://webftp.gazi.edu.tr/hukuk/dergi/14_2_10.pdf, ET. 5 Mart 2020.
795 A.e., s. 286.
796 A.e., s. 291.

"Madde 303a- (1) Hukuka aykırı olarak (202a maddesi ikinci fıkrası anlamındaki) verileri silen, gizleyen, kullanılmaz hale getiren veya değiştiren kişi, iki yıla kadar hapis veya (adli) para cezası ile cezalandırılır.

(2) Bu suça teşebbüs cezalandırılır.

(3) Birinci fıkrada tanımlanmış bulunan suça hazırlık hareketleri hakkında, 202c maddesi, gereğince uygulanır."[797]

"Bilgisayar sabotajı":

"Madde 303b- (1) Bir başkası için önemi olan veriye dayalı bir işlemi 1. 303a maddesi birinci fıkrasındaki suçu işlemek, 2. 202a maddesi ikinci fıkrası anlamındaki verileri, başkasına zarar vermek maksadıyla bilgisayara girmek veya iletmek ya da 3. bir bilgi işlem sistemini veya işlemciyi bozmak, zarara uğratmak, kullanılmaz hale getirmek, yok etmek veya değiştirmek suretiyle önemli derecede bozan kişi, üç yıla kadar hapis veya (adli) para cezası ile cezalandırılır.

(2) Bir başkasına ait bir işletme, kuruluş veya kurum için önemli olan veriye dayalı bir işlemin söz konusu olması halinde ise ceza beş yıla kadar hapis veya (adli) para cezasıdır.

(3) Bu suça teşebbüs cezalandırılır.

(4) İkinci fıkranın nitelikli hallerinde ceza altı aydan on yıla kadar hapis cezasıdır. Failin, 1. önemli derecede bir malvarlığı kaybına sebebiyet vermesi, 2. suçu, meslek edinerek veya bilgisayar sabotajı suçunu sürekli şekilde işlemek amacıyla kurulmuş bulunan bir örgüte üye olarak işlemesi, 3. bu suçun işlenmesi neticesinde, halkın ihtiyaçları için yaşamsal önemdeki besin, mal veya hizmetlerin karşılanması ya da Almanya Federal Cumhuriyeti'nin güvenliğinin zarar görmesi durumlarında kural olarak nitelikli hal vardır.

(5) Birinci fıkradaki suça hazırlık hareketleri için 202c maddesi, gereğince uygulanır."[798]

"Veri Casusluğunun ve Verilerin İletilirken Ele Geçirilmesinin Hazırlığı" başlıklı 202c m.' si ise:

"(1) Her kim 202a veya 202b maddelerde belirtilen suçların işlenmesini hazırlamak üzere, 1. Verilere giriş yapmayı sağlayan (m. 202a fıkra 2) şifre ve sair güvenlik kodlarını veya, 2. Bu tür fiilleri işlemeyi amaçlayan bilgisayar programlarını, üretir,

797 A.e., s. 292.
798 A.e., 293.

kendisine veya bir başkaına sağlar, satar, bir başkasına verir, yayar veya sair bir şekilde ulaşılabilmesini sağlarsa, bir yıla kadar hapis cezası veya adli para cezası ile cezalandırılır."[799]

Yine Alman Ceza Kanunu' nda "dolandırıcılık ve güveni kötüye kullanma" bölümünde düzenlenen 266b m.' si ve "para ve kıymetli damgalarda sahtecilik" bölümünde düzenlenen 152a m.' si ve 152b m.' si hükümleri TCK 245. m.' dekilere benzer düzenlemeler içermekte olup TCK' dan farklılık gösteren Alman temel Ceza Kanunu' nda, bilişim alanında suçlar bölümü altında bütün olarak ele alınmak yerine Kanun'un farklı bölümlerimde ve ayrı hükümler içerisinde düzenlenmiştir.[800]

799 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 238.

800 Erdağ, a.g.e., s. 297, 300.

"Çek ve kredi kartlarının kötüye kullanılması Madde 266b- (1) Kendisine bir çek veya kredi kartının bırakılmasıyla ele geçirdiği, kart düzenleyicisini bir meblağı ödemeye zorlama imkanını, kötüye kullanan ve düzenleyiciyi bu surette zarara uğratan kişi üç yıla hapis veya (adli) para cezası ile cezalandırılır.

(2) 248a maddesi84, bu madde bakımından da (gereğince) uygulanır." Bkz. a.e., s. 298.

"Ödeme kartlarında, çeklerde ve senetlerde sahtecilik Madde 152a- (1) Hukuki ilişkilerde aldatmak veya böyle bir yanıltmayı mümkün kılmak için, 1. yerli veya yabancı menşeli ödeme kartlarını, çekleri ya da senetleri sahte olarak üreten veya değiştiren ya da 2. bu türden sahte kartları, çekleri veya senetleri kendisi ya da başkası için temin eden, satan, bir başkasına devreden veya kullanan kişi, beş yıla kadar hapis veya (adli) para cezası ile cezalandırılır.

(2) Bu suça teşebbüs cezalandırılır.

(3) Fail, suçu meslek edinerek veya birinci fıkradaki suçu sürekli şekilde işlemek amacıyla kurulmuş bulunan bir örgüte üye olarak hareket ederse ceza altı aydan on yıla kadar hapis cezasıdır.

(4) 1. Bir kredi kurumundan veya mali alanda hizmet veren bir kurumdan verilen kartlar ve 2. donanımı veya kodlanması suretiyle sahteciliğe karşı özel olarak korunan kartlar birinci fıkra anlamında ödeme kartıdır.

(5) Kıymetli damgalarda sahtecilikle ilgili olmak kaydıyla 149. madde 89 ile 150. maddenin ikinci fıkrası 90, bu madde bakımından da (gereğince) uygulanır." Bkz. a.e., s. 299, 300.

"Garantili ödeme kartlarında ve Euro-çek formlarında sahtecilik Madde 152b- (1) 152a maddesinin birinci fıkrasında belirtilen fi illerden birini garantili ödeme kartları veya Euro-çek formları hakkında işleyen kişi bir yıldan on yıla kadar hapis cezası ile cezalandırılır.

(2) Fail, suçu meslek edinerek veya birinci fıkradaki suçu sürekli şekilde işlemek amacıyla kurulmuş bulunan bir örgüte üye olarak hareket ederse hapis cezası iki yıldan az olamaz.

(3) Birinci fıkranın nitelikli hallerinde üç aydan beş yıla kadar, ikinci fıkranın nitelikli hallerinde ise bir yıldan on yıla kadar hapis cezasına hükmolunur.

(4) 1. düzenleyicisinin iş yaşamında bir ödemeyi garantili olarak yapmasını zorunlu kılan ve 2. donanımı veya kodlanması suretiyle sahteciliğe karşı özel olarak korunan kredi kartları, Euro-çek kartları ya da diğer kartlar birinci fıkra anlamında garantili ödeme kartıdır.

(5) Parada sahtecilikle ilgili olmak kaydıyla 149. madde ile 150. maddenin ikinci fıkrası, bu madde bakımından da (gereğince) uygulanır." Bkz. a.e., s. 300.

Yine aynı Kanun' un "263a m.' sinde"[801] bilişim sistemi aracılığıyla dolandırıcılık fiilleri, "269 ve 279. m.' lerinde"[802] ise bilişim sistemleri aracılığıyla sahtekarlık fiilleri suç olarak düzenlenmiş[803], 176. ve 184d m.' lerinde ise çocuk pornografisine ilişkin düzenlemeler yer almıştır.[804]

13 Temmuz 1997 yılında kabul edilen Teleservisler Kanunu ile internet yayınlarından doğan ceza sorumluluğunun esasları belirlenmiş[805] başka bir deyişle internet süjelerinin sorumluluğu konusunda düzenlemeler yapılmış[806], buna göre internetteki herhangi bir yayının içeriğini hazırlayan içerik sağlayıcı, o yayında yer alan yazı, resim ve diğer materyaller suç unsuru taşıyor ise genel hükümlere göre sorumlu olacak, erişim sağlayıcılarının ise cezai sorumluluğu bulunmayacak, servis sağlayıcılar ana bilgisayarda depoladıkları başkalarına ait suç içerikli bilgilerin bu niteliğinden haberdar olmaları ve ayrıca bu bilgilerin internet üzerinden erişilebilir kılınmasını teknik olarak önleme olanağına sahip bulunmaları halinde bu bilgilere erişimi önlememeleri halinde belirtilen ihmali davranışından dolayı sorumlu tutulabilecekleri düzenlenmiştir.[807] Son olarak söz konusu Kanun' da 14.12.2001 yılında yapılan değişiklik ile internet kişilerinin sorumluluk alanları genişletilmiştir.[808]

---

801 "Dolandırıcılık suçlarında, kendisinin veya üçüncü kişinin malvarlığında hukuka aykırı bir artış sağlama amacıyla bilgisayarı hatalı bir sonuç verecek şekilde programlayan veya bir şekilde yetkisiz olarak bilgisayar programının işleyiş sürecine müdahale eden kişi 5 yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu amacı taşıyan bilgisayar programlarını imal veya temin eden, satışa sunan, bulunduran veya başkasına bırakan kişi ise 3 yıla kadar hapis veya adli para cezası ile cezalandırılır." Bkz. Karagöz, a.g.e., s. 98.

802 "Sahtecilik suçlarında, ispat değeri taşıyan verileri aldatma amacıyla kayıt eden, değiştiren veya bu şekilde bulunan verileri kullanan kişi 5 yıla kadar hapis veya adli para cezası ile cezalandırılır." Bkz. a.e.

803 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 219, 220.

804 "Çocukların cinsel istismarında, bilişim teknolojisi kullanılarak veya bu teknolojiler ile pornografik içerikleri ulaşılabilir hale getirerek çocuğu cinsel davranışlarda bulunmak amacıyla etkileyen kişi 3 aydan 5 yıla kadar hapis cezası ile cezalandırılır. (176)

Pornografik içeriğe radyo veya telekomünikasyon medyaları yoluyla hukuka aykırı şekilde bir başka kişinin veya kamunun erişimini sağlayan kişi 184 ila 184c maddeleri uyarınca cezalandırılır. Telekomünikasyon medyaları aracılığıyla çocuk pornografisi konulu bir içeriğe erişmeye girişen kişi 184b maddesi uyarınca, genç pornografisi konulu bir içeriğe erişmek isteyen kişi ise 184c maddesi uyarınca cezalandırılır." Bkz. Karagöz, a.g.e., s. 97, 98.

805 Eryaman, a.g.e., s. 44.

806 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 59.

807 Kurt, a.g.e., s. 107, 108; Nacar, a.g.e., s. 28.

808 Nacar, a.g.e., s. 29.

"…Alman yasa koyucusu, Avrupa Parlamentosu'nun ve Konseyinin 08.06.2000 tarihli ve 2000/31 sayılı Direktifini de dikkate alarak 14.12.2001 tarihinde Teleservisler Kanunu'nda değişiklikler yapmış, bununla sorumluluk bölümü genişletilmiş, yeni ve daha ayrıntılı bazı esaslar benimsenmiştir." Bkz. *Erdoğan, Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 59.

2.2.4. İtalya

İtalyan Ceza Kanunu ve Ceza Usul Kanunu' nda 23.12.1993 tarihli ve 547 sayılı Kanun ile yapılan değişiklikle Ceza Kanunu' nun çeşitli maddelerine bilişim alanında gerçekleştirilen çoğu fiil suç olarak düzenlenip eklenmiştir.[809] Yapılan bu değişikliklerde, 1930 Rocco Ceza Kanunu' nda öngörülen "hukuki yarar" kriteri ile oluşturulan sistematik bozulmadan ayrı bir düzenlemeye gidilmeyerek mevcut suçların içerisinde değişiklikler yapılmış, ancak bilgisayarla işlenen eylemleri karşılamak bakımından ceza kanununda mevcut suçların yetersiz kalması halinde komisyon yeni suçlar ihdas etmiştir.[810]

"Bilgi teknolojileri veya telematik sistemlere yetkisiz erişim"[811] (m. 615-ter), "Bilgisayar veya telekomünikasyon sistemleri giriş kodlarının yasadışı yayılması"[812] (m. 615-quater), "Bilgi teknolojileri veya telematik sistemleri kesen veya onlara zarar veren malzeme, cihaz veya bilgisayar programlarının yayılması"[813] (m. 615-quinquies), "Veri, bilgi veya bilgisayar programlarına zarar verilmesi"[814] (m. 635-bis), "Kamu bünyesinde veya kullanımında bulunan veri, bilgi veya bilgisayar programlarına zarar verilmesi"[815] (m. 635-ter), "Bilgi sistemleri veya telematik

809 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 219, 222.
810 Kurt, a.g.e., s. 104.
811 "(1) Güvenlik önlemleri ile korunan bir bilgi teknolojileri sistemi veya elektronik sisteme kendisini uygunsuz şekilde tanıtan (bu şekilde giren) veya kendisini çıkarma yetkisine sahip kişilerin açık veya zımni niyetine karşı sistemde kalmaya devam eden kişi 3 yıla kadar hapis cezası ile cezalandırılır. (2) Eylemin 1) Kamu görevlisi veya kamu hizmetlerinden sorumlu kişinin görevini kötüye kullanarak, 2) Fail tarafından nesnelere veya kişilere cebir uygulanarak veya silahlı halde, 3) Eylem, sistemin, verinin veya programlarının tamamının veya bir bölümünün yok edilmesi, zarar görmesi veya engellenmesi ile sonuçlanırsa 1 yıldan 5 yıla kadar hapis cezası verilir. (3) Eğer bu bölümdeki eylemlerin askeri alanı, toplum düzenini, kamu güvenliği, sağlığını veya yararını ilgilendirmesi halinde sırasıyla (fıkralara göre) 1 yıldan 5 yıla kadar ve 3 yıldan 8 yıla kadar ceza verilir. (4) Birinci fıkra kapsamındaki suçlar şikâyete tabiidir." Bkz. Karagöz, a.g.e., s. 104.
812 "Kendisine veya bir başkasına yarar sağlamak veya başkasına zarar vermek için, telematik sistemlere giriş için uygun olan ve korunan kodları sakıncalı şekilde sağlayan, çoğaltan, yasadışı yayan veya veren kişi 1 yıla kadar hapis ve 5164 €'ya kadar para cezası ile cezalandırılır." Bkz. a.e.
813 "Bilgi teknolojileri sistemleri, bilgi, veri veya bilgisayar programlarının bir kısmına veya tamamına yasadışı şekilde zarar vermek amacıyla, başkaca ekipman veya bilgisayar programlarını üreten, temin eden, yayan veya başka bir şekilde kullanıma uygun hale getiren kişi 2 yıla kadar hapis ve 10.329 €'ya kadar para cezası verilir." Bkz. a.e., s. 104, 105.
814 "Eylem daha ağır bir cezayı gerektirmediği takdirde, veri veya bilgisayar programını yok eden, bozan, silen, değiştiren veya durduran kişi hakkında mağdurun şikâyeti üzerine 6 aydan 3 yıla kadar hapis cezası verilir. Eylem, sistem operatörünün kötüye kullanımıyla gerçekleşmiş ise şikâyet aranmaksızın 1 yıldan 4 yıla kadar hapis cezası ile cezalandırılır." Bkz. a.e., s. 105.
"…başkasının bilişim sistemini, yazılımlarını veya verilerini tamamen veya kısmen yok etme, tahrip etme veya kullanılamaz hale getirme suçudur. Bu maddeyle bilişim veya telematik sistemlerinin veya bilişim programlarının veya verilerinin özel tahrip hali suç olarak düzenlenmektedir." Bkz. Erdoğan, Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle), s. 62.
815 "Eylem daha ağır bir cezayı gerektirmediği takdirde, herhangi bir şekilde kamu bünyesi veya kullanımında olan veri, bilgi veya bilgisayar programını yok eden, zarar veren, değiştiren veya durduran kişi 1 yıldan 4 yıla kadar hapis cezası ile cezalandırılır. Eylem yok etme, zarar verme,

sistemlere zarar verilmesi"[816] (m. 635-quater), "Kamu kullanımında olan bilgi sistemleri veya telematik sistemlere zarar verilmesi"[817] (m. 635 quinquies), "Kişisel nedenlerle keyfi uygulama sonucu mala zarar verme"[818] (m. 392), "Sahte para, damga pulu veya filigran üretme veya bulundurma"[819] (m. 461), "Gizli doküman içeriklerinin açığa çıkarılması"[820] (m. 621) suçları düzenleme konusu suçlardan bazılarıdır. Yine Kanun' un 392. m.' sinin 3. fıkrasında "bir bilişim programını tamamen veya kısmen tahrip etmek, değiştirmek, silmek veya bilişim ya da telematik sistemin işlemesini engelleme veya bozma" ve 420. m.' sinin 2. fıkrasında "kamusal yarar bulunan bilişim veya telematik sistemlere zarar verme veya yok etmeye yönelik" eylemler suç olarak düzenlenmiştir.[821]

Yine Kanun' un 640ter m.' sinde, "bilişim sistemi aracılığı ile dolandırıcılık suçu"[822], 600ter m.' sinde ise küçüklerin pornografik materyallerde kullanılması suçunun internet aracılığıyla işlenmesi, 491bis m.' sinde ise "bilişim belgelerinde yapılan sahtecilik"[823] fiili suç olarak düzenlenmiştir.[824]

---

değiştirme, silme veya durdurma ile sonuçlanmış ise 3 yıldan 8 yıla kadar hapis cezası verilir. Eylem, sistem operatörünün kötüye kullanımıyla gerçekleşmiş ise verilecek ceza arttırılır." Bkz. Karagöz, a.g.e., s. 105.

816 "Eylem daha ağır bir cezayı gerektirmediği takdirde, 635-bis maddesindeki eylemleri gerçekleştirerek veya veri aktarımı-bulaştırması yoluyla bilgi teknolojisi veya diğer telekomünikasyon sistemlerinin bütününü veya bir parçasını kullanılamaz hale getiren veya fonksiyonlarını ciddi şekilde geciktiren kişi 1 yıldan 5 yıla kadar hapis cezası ile cezalandırılır. Eylem, sistem operatörünün kötüye kullanımıyla gerçekleşmiş ise verilecek ceza arttırılır." Bkz. a.e.

817 "635-quater maddesinde belirtilen eylemlerin kamu kullanımında olan bilgi sistemleri veya telematik sistemlerin bütünü veya bir bölümüne gerçekleştiren kişi 1 yıldan 4 yıla kadar hapis cezası ile cezalandırılır. Eylem, sistemlerin yok edilmesi, zarar verilmesi veya kullanılamaz hale getirilmesi ile sonuçlanırsa fail hakkında 3 yıldan 8 yıla kadar hapis cezası verilir. Eylem, sistem operatörünün kötüye kullanımıyla gerçekleşmiş ise verilecek ceza arttırılır." Bkz. a.e.

818 "Mahkemeye başvurarak iddia ettiği haklarını kullanabilecek olan kişi, hakkı keyfi olarak kendi kullanıp mala zarar verdiği takdirde, şikayetçinin davası ile 516 €'ya kadar para cezası ile cezalandırı-lır. Bu kapsamda bir bilgi teknolojileri programının bütününün veya bir bölümünün değiştirilmesi, modifiye edilmesi, kaldırılması veya telekomünikasyon sistemlerinin engellemesi veya aksatılması da mala zarar verme sayılır." Bkz. a.e., s. 105, 106.

819 "Eylem daha ağır bir cezayı gerektirmediği takdirde, sahte para, pul veya filigranlı kâğıt elde etmek için, filigran, bilgisayar programı veya materyal imal eden, satın alan, bulunduran veya devreden kişi 1 yıldan 5 yıla kadar hapis ve 103 – 516 € para cezasına çarptırılır." Bkz. a.e., s. 106.

820 "İçerikten habersiz olarak, gizli kalması gereken içerikleri kendi çıkarına veya herhangi bir sebep olmaksızın kullanan kişi, 3 yıla kadar hapis veya hapis ile birlikte 103 – 1032 € arasında para cezasına çarptırılır. Bu kapsamda, bilişim teknolojileri kapsamındaki her türlü veri, bilgi veya program da suçun konusu içerik olarak varsayılır." Bkz. a.e.

821 Kurt, a.g.e., s. 105.

822 "Bir bilişim sistemini veya telematik sistemin işlemesini herhangi bir şekilde değiştirerek veya bu tür sistemlerdeki veri veya programlara hukuka aykırı şekilde müdahale ederek başkasının zararına veya başkasının yararına haksız kazanç elde edilmesi suç sayılmış bu suçun basit hali suçta zarar görenin şikayeti üzerine kovuşturmaya tabidir." Bkz. Nacar, a.g.e., s. 27.

823 Kanun' un aynı maddesinde "bilişim belgesi", "ispat etkisi olan veri veya bilgileri ya da bunları özel olarak oluşturmaya yönelik programları içeren kayıt" olarak ifade edilmiştir. Bkz. A.e., s. 222, 223.

824 A.e., s. 222, 223.

Kanun' un 617 quarter m.' sinde ise "Bilişim veya Telematik Haberleşmenin Dinlenmesi, Engellenmesi veya Araya Girilmesi" suç olarak düzenlenmiş olup suçun ağırlaştırıcı nedenleri ise; suçun devlet, kamu kuruluşu veya kamu hizmeti gören kuruluşların kullandığı bilişim sistemi veya telematik bir sistem zararına işlenmiş olması, bir kamu görevlisi veya hizmetlisinin görev ve yetkilerini kötüye kullanarak veya sistem operatörlerinin bu sıfatlarını kötüye kullanarak işlemesi veya özel dedektiflik yetkisinin kötüye kullanılarak işlenmesi olarak belirlenmiştir.[825]

Yukarıda incelemiş olduğumuz İtalyan Ceza Kanunu m.' lerinin yanında mafya türü örgütlü suçlulukla mücadele parçası olarak suç gelirlerinin aklanması suçuyla etkin mücadele edilebilmesi için 356/1992 sayılı Kanun kabul edilerek bilişim sistemlerini de kapsamak suretiyle suç gelirlerinin aklanması suçunda hazırlık hareketlerinin dahi cezalandırılması öngörülmüştür.[826]

2.2.5. İngiltere

Anglo Sakson hukuk sistemi içerisinde yer alan İngiltere' de de bilişim suçları ayrı kanunlar içerisinde düzenlenmiştir.[827] Bu yasalar 29.8.1990 tarihli Bilgisayarların Kötüye Kullanılması Kanunu, 1907 tarihli Bermuda Ceza Kanunu, 1959 tarihli Müstehcen Yayınlar Kanunu, "1978 tarihli Çocuk Koruma Kanunu"[828], "1981 tarihli Sahtecilik ve Kalpazanlık Yasası"[829], 1988 tarihli Telif, Tasarım ve Patent Kanunu,

825 Nacar, a.g.e., s. 26, 27.
826 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 63; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 224; Karagöz, a.g.e., s. 106; Nacar, a.g.e., s. 28.
827 Kurt, a.g.e., s. 102.
828 "İngiltere'de, 1978 tarihli "Çocukların Korunması Kanunu'nda" yer alan "fotoğraf" tanımı, 1994 tarihli "Ceza Adaleti ve Kamu Düzeni Kanunu" ile sanal alanda sayısal formda veri halinde bulunan resimleri de kapsayacak şekilde değiştirilmiş, böylelikle internette veri halinde bulunan çocuk pornografisi resimleri ve bunların montajla yapılmış şekillerini bulundurmak suç haline getirilmiştir." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 221.
829 "Siber alanda failler, geniş kaynaklardan elde ettikleri bilgileri kullanarak, yeni haklar oluşturabilecekleri gibi sahte belgeleri kullanarak mevcut hakları da istismar edebilirler. Bu bilgiler, sosyal mühendislik teknikleri kullanılmak suretiyle mağdurların kendilerinden elde edilmektedir; zira insanların bilgilerini açıklamaları için yine insanlar tarafından gerçekleştirilen hileli hareketler, veri güvenliği için getirilen mekanizmaların ve prosedürlerin üstesinden gelinmesinde yardımcı olmaktadır. Bu tekniklerin başarısı kısmen insanların internet üzerinden mahrem bilgilerini açıklamaya hazır olmalarından (örneğin, sosyal arkadaşlık sitelerinde olduğu gibi dolayı kolay olmaktadır. Bu alandaki bir başka seçenek ise failin, bir elektronik ticaret sitesinin müşteri veri tabanının güvenliğini kırarak kredi kartı bilgilerini ve müşterilere ait diğer belgeleri ele geçirmesidir. Bu her iki hareket de İngiliz hukukunda 1981 tarihli Sahtecilik ve Kalpazanlık Yasası Forgery and Counterfeiting Act 1981) gereğince suç oluşturmaktadır." Bkz. Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 179.

1998 tarihli Veri Koruma Kanunu, "2003 tarihli Cinsel Suçlar Kanunu"[830], "2006 tarihli Dolandırıcılık Kanunu"[831], 2006 tarihli Terörizm Kanunu ve 2008 tarihli Tüketicilerin Haksız Ticaretten Korunması Düzenlemesi Kanunlarıdır.[832] Doktrinde yer alan bir görüşte, Birleşik Krallıkta ve esasen tüm dünyada büyük ve ciddi bir sorun olan internetin sağladığı kolaylıktan yararlanmak suretiyle çocukla kurulabilecek iletişimin kolaylaşması sonucunda çocuklara yönelik taciz oluşturan hareketlere rıza göstermeleri amacıyla çocukların güvenini kazanmaya yönelik aktivitelerin her gün giderek artan çocuk istismarları olayları karşısında ülkemiz mevzuatında tekrar gözden geçirilmek suretiyle düzenlenmesi gerektiği[833], siber ortamın siyasal sınırlarının

830 "…Bu tür aktivitelerle mücadele etmek için, 2003 tarihli Cinsel Suçlar Yasası (Sexual Offences Act 2003) ile "cinsel 'grooming'e yönelik çocukla tanışma" suçu düzenlenmiştir. Söz konusu suç şu hareketleri düzenlemektedir:
"Bir kişi (A) bir başka kişi (B) ile bir ya da daha fazla ortamda iletişime geçer ya da görüşürse ve devamında –
(i) A kasten B ile görüşürse,
(ii) A, B ile görüşmek kastıyla dünyanın herhangi bir yerine seyahat ederse ya da dünyanın herhangi bir yerinde B ile görüşmek için ayarlama yaparsa veya,
(iii) B, A ile görüşmek için dünyanın herhangi bir yerine seyahat ederse…"…" bkz. A.e., s. 192, 193.
"2015 yılında, 2003 tarihli Cinsel Suçlar Yasası'na "çocukla cinsel konulu iletişim kurulması suçu" eklenmiştir. İletişimin içeriği, mantıklı bir insanın kabul edebileceği bir şekilde "cinsel aktivite" ile ilgili olmak zorundadır. İletişim, yetişkin bir kişi ile on altı yaşından küçük bir çocuk arasında gerçekleşmelidir. Bu suçun cezası azami iki yıl hapis cezasıdır, ayrıca not edilmesi gereken ilginç bir husus da, düşünce açıklama ile ilgili diğer suçlardan farklı olarak, bu suçun soruşturulması için başsavcılığın (Director of Prosecutions) iznini gerektirmemesidir." Bkz. A.e., s. 194.
831 "…Sonuçta 2006 tarihli Dolandırıcılık Yasası (The Fraud Act 2006) ile internet servislerinden sahtecilikle ve aldatmayla hizmet alınması suç haline getirilmiştir.
Bu yasadaki suç tanımıyla birlikte, suçun oluşması için yasada yazılı olmayan diğer üç unsurun da bulunması gerekir. Bunlardan ilki verilen hizmetin şartlarına odaklanmıştır; buna göre hizmet ücret karşılığı verilmiş ya da verilecek olmalıdır. İkinci unsur, fail bu ücreti ödemeksizin hizmeti almış olmalıdır. Üçüncü unsur ve suçun ikinci manevi unsuru ise, fail bu hizmetin elde edilebilir ya da elde edilebilecek olduğunu bilmeli ancak ödeme yapma niyetinde olmamalıdır." Bkz. A.e., s. 178.
832 Karagöz, a.g.e., s. 102.
833 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 192, 193.
"…internet, pedofillerin çocuk istismarı amacıyla çocuklarla iletişime geçebilmeleri için yeni olanaklar sağlamıştır; işte buna "internet grooming" adı verilmektedir. Bu tür aktivitelerde internet, çocuklar ile iletişim kurmak ve onların güzellikle ikna edilebilmeleri için bir aracı olarak kullanılmaktadır.
…Geniş bir biçimde kullanılan "grooming" terimi, ne tam olarak açıklanabilen ne de tanımlanabilen karmaşık bir olguyu belirtir. Grooming'in aşamaları şunlardır: a) Çeşitli manipülatif ya da kontrol edici tekniklerin kullanılması, b) Kırılgan bir mağdurun bulunması, c) Kişiler arası ve sosyal kurguların olması (belli bir kapsamda) d) Zarar verici seksüel davranışların normal gösterilmesi için güven otamının oluşturulması, e) İstismarı kolaylaştırmak için ve/veya ortaya çıkmasını engellemek için tüm bu sayıların gerçekleştirilmesi." Bkz. A.e., s. 191, 192.
"Teknolojinin gelişmesi ve gündelik hayatımızda kalıcı bir yer edinmesi ile birlikte çocuk istismarının bazı boyutları sanal mekanlara taşınmaya başlandı. İnternetin veya sanal ortamın, anonim hareket etmeyi de mümkün kılması, failin daha rahat ve kendi gibi olmadan hareket etmesi burada en önemli notalardandır. Dahası faillerin yakalanmayacaklarını düşünmeleri de bazı suçlar yönünden suç yeri olarak interneti tercih etmelerinde etkilidir.
Çocukların, sanal ortamda kötü niyetli kişilerin hedefi haline gelerek iletişime geçilmeye çalışılması günümüzde ciddi bir tehlike arz eder ve bu duruma siber uşaklaştırma / grooming denilir.

olmaması, dünyanın her yerinden kişilerin bu ağa katılarak iletişim kurabilmeleri gibi sebeplerle dünyanın her yerinde problem olarak karşılaşılan "grooming"[834] adı verilen aktivitelerle ilgili olarak uluslararası alanda yapılan araştırmalar çocukların ciddi bir risk altında bulunduğunu göstermekte ise de (10-17 yaş aralığındaki çocukların %13 ila %19'unun cinsel taleplere maruz kaldığı belirtilmiş) ülkemizde bu sürece yönelik herhangi bir yasal düzenleme bulunmamakla birlikte uluslararası alanda kimi ülkelerin yasal düzenlemeler getirdiği belirtilmektedir.[835]

… Ancak bu kavram ülkemiz açısından bilinen ve farkındalığı olan bir kavram değildir. Ülkemiz bu kavramla daha çok yeni tanışmıştır.

… Siber uşaklaştırma denilen kavram mağdura erişim ile başlayan ve belirli bir süreç neticesinde istismar eylemi ile biten stratejilerin bir kısmı, eş deyişle mağduru istismara hazırlama süreci olarak tanımlanmıştır . Yine siber uşaklaştırma evrensel olarak saldırganın fantezilerini gerçeğe döktüğü bir teknik olarak da anlaşılmaktadır . Başka bir tanımla siber uşaklaştırma, çocuk istismarcılarının gelecekteki kurbandan yararlanıp onları istismarla uyumlu hale getirmek için hazırladıkları taktiklerdir . Bennett ve O'Donohu ise cinsel istismar olasılığını artırmak için işlev gören uygunsuz davranış olarak tanımlamaktadır . Michael Welner'e göre siber uşaklaştırma saldırgan tarafından mağdurun cinsel ilişkiye sürüklendiği ve bu ilişkinin gizli şekilde yürütüldüğü bir süreçtir . Siber uşaklaştırma genellikle çevrim içi sohbet odalarının kasıtlı olarak kullanılması ile başlamaktadır. Bu yol ile çocuk istismar edilmek üzere uşaklaştırılmakta ve istismara hazırlanmaktadır . Saldırgan bu sürece başlayarak mağdura nasıl ulaşacağı ile en kolay ne şekilde istismar edeceğini ve cinsel teması sağlayacağını belirlemektedir. Saldırgan bu süreci izlerken en uygun zamanı beklemekte ve belirli yöntemlerle, aşamalarla çocuğu etkilemeye çalışmaktadır.

… Avrupa Çevrimiçi Çocuklar Araştırma Projesi'ne (Türkiye) göre çocukların %42'si interneti kişisel bilgilerini herkese açık olarak kullanmaktadır. Türkiye'de 9-16 yaş aralığındaki çocukların %45,9'u 7-10yaş aralığında internet kullanmaya başlamaktadır. Hatta Türkiye'de çocukların %32,2'si kendi masaüstü bilgisayarından internete bağlanmaktadır . Türkiye İstatistik Kurumu'nun (TÜİK) 2013 yılında yaptığı araştırmaya göre 6-15 yaş aralığındaki çocukların interneti kullanmaya başlama yaşı ortalama 9(dokuz)'dur . Avrupa Çevrimiçi Çocuk Araştırması çocukların bu kötü niyetli davranışlarla karşılaştığını göstermektedir. Buna göre 10-17 yaş aralığındaki çocukların %13 ila %19'u cinsel taleplere maruz kalmaktadır . Türkiye'de ise çocukların %11,5'i cinsel içerikli mesaj almaktadır . Yine Avrupa Çevrimiçi Çocuk Araştırmasına göre Türkiye'de ebeveynlerin yalnızca %28,6'sı internet kullanmaktadır . Türkiye'de ebeveynlerin yalnızca %33,6'sı bilgisayarlara filtre programı kurmaktadır…" bkz. Oğuz Polat, "Çocuk İstismarında Farklı Bir Kavram: Grooming (Siber Uşaklaştırma) ve Türkiye", Şiddeti Önleme ve Rehabilitasyon Derneği - Acıbadem Mehmet Ali Aydınlar Suç ve Şiddetle Mücadele, *Uygulama ve Araştırma Merkezi Basın Özeti*, s. 1, 2, 6, 7, 11, http://imdat.org/wp-content/uploads/2019/04/Prof.-O%C4%9Fuz-Polat-23-Nisan-Grooming-Rapor.pdf, ET. 10 Mart 2020.

834 "Grooming, bir kişinin cinsel istismar fiilini gerçekleştirmeye hazırlık yapmak için çocukla internet ortamında cinsel içerikli sohbet etmesi olarak tanımlanmaktadır. Diğer bir ifadeyle çocuklara cinsel istismarda bulunmak amacıyla onlarla bilişim ve iletişim teknolojileri yoluyla arkadaşlık kurmak, güven kazanmak ve buluşarak fiziksel istismarda bulunmaya çalışmak olarak ifade edilmektedir. Bu arkadaşlık, çocuk ile cinsel bir etkinlik gerçekleştirmeyi sağlayabilmek için kurulan duygusal arkadaşlık bağını ifade etmektedir. Ayrıca bu fiilin, çocuklara cinsel etkinlikleri ve çocuk pornografisini özendirmek amacıyla kullanıldığı görülmektedir. Grooming birbirinden farklı çocuklara yönelik suçların hazırlık hareketi olarak değerlendirildiğinden birçok ülkede suç olarak kabul edilmiştir." Bkz. Kara ve Kaya, a.g.e., s. 162.

835 "Avustralya

Avustralya'da 9-16 yaşlarındaki 400 çocuk ile ailelerinden biri ile yapılan çalışmada çocukların ortalama 8 yaşında interneti kullanmaya başladığı, %76'sının her gün çevrimiçi olduğu, her üç çocuktan birinin son bir yılda çevrimiçi olarak rahatsız edildiği, çocukların %34'ünün yüz yüze görüşmedikleri biriyle internet üzerinden konuştuğu, %5'inin ise bu kişilerle buluştuğu tespit edilmiştir . Bunun yanında siber uşaklaştırmaya yönelik düzenleme de yapılmıştır. Avustralya Ceza Kanununa göre 16 yaşından küçük bir kişiyi temin etme niyetiyle iletişim kurmak için "taşıyıcı hizmet "kullanımı ile böyle bir kişiyi siber uşaklaştırma amacıyla uygun olmayan herhangi bir şeye

Bilişim suçları alanında temel yasa olarak kabul edilebilecek olan 29.8.1990 tarihli Bilgisayarların Kötüye Kullanılması Kanunu' nun 1. m.' sinde temel suç olarak

maruz bırakmayı suç olarak düzenlemiştir. Ancak bazı eyaletler 18 yaşından küçük olmayı yeterli görmüştür .

İsveç

Avrupa Çevrimiçi Çocuk Araştırmasına göre İsveçli çocuklar Avrupa ülkeler arasında en erken yaşta internet kullanmaya başlayanlardır. Buna göre interneti kullanmaya 19 başlama yaşları 7'dir. Aynı zamanda İsveç, Avrupa'da en fazla internetin kullanıldığı ülkelerden biridir. Başka bir araştırmaya göre, on beş yaşındaki kızların% 48'i, erkeklerin% 18'i çevrimiçi olarak cinsel taleple karşı karşıya kalmıştır . İsveç'te yaşanan en büyük siber uşaklaştırma olayı Alexandra davasıdır. Olayda Alexandra takma ad kullanarak, mağdurlarla güven ilişkisi kurmuş ve bu şekilde mağdurların direncini kırmış, sonrasında ise mağdurların istismar eylemini kimseye söylememelerini sağlamıştır . Yaşanan olaydan sonra 1 Temmuz 2009'da İsveç Ceza Kanunu'nda değişiklik yapılarak cinsel amaçla çocuk ile irtibat kurmak suç olarak düzenlenmiştir.

İngiltere

Avrupa Çevrimiçi Çocuk Araştırmasına göre İngiltere'de çocukların %70'i her gün interneti kullanmakta ve %29'u daha önce yüz yüze görüşmediği kişilerle çevrimiçi olarak görüşmekte, %4'ü ise bu kişilerle gerçek yaşamda buluşmaktadır . Birleşik Krallıkta iki polis amirliği tarafından elde edilen verilere göre adli vakaların %2.1'inin siber uşaklaştırma ile bağlantılı olduğu belirtilmiştir. Aynı zamanda Birleşik Krallıkta 1 Nisan 2009 ile 31 Mart 2010 tarihleri arasında yapılan bildirimlerin %66'sının siber uşaklaştırma ile ilgili olduğu tespit edilmiştir. İngiltere'de siber uşaklaştırmaya yönelik yapılan yasal düzenlemeye göre bir yetişkin, istismar amacıyla çocukla bir araya gelir ya da iletişime geçerse (bilgisayar tabanlı iletişim) bu durum suç teşkil eder.

Kanada

Kanada Ceza Kanuna göre bir çocuğun cinsel bir suç işlemesi amacıyla bir bilgisayar sistemi aracılığıyla iletişim kurulması suç teşkil eder.

Kosta Rika

Bir çocuğun elektronik vasıtalar kullanılarak baştan çıkarılması suç olarak düzenlenmiştir. Hollanda Hollanda Ceza Yasasına göre 16 yaşın altındaki bir çocuğun siber uşaklaştırılması suç olarak kabul edilmiştir.

Amerika Birleşik Devletleri

Amerika Birleşik Devletlerinde herhangi bir kişinin küçük birisini cinsel aktiviteye ikna etmek için postaları, eyaletler arası ticareti vb. kullanması federal suç olarak düzenlenmiştir. Ayrıca 16 yaşın altındaki bir kişi hakkında bilgi iletmek de federal suç teşkil etmektedir." Bkz. Polat, a.g.e., s. 18, 19.

"Durum o kadar vahimdir ki internetteki çocuk pornografisi ile ilgili olabilecek 12 anahtar sözcük kullanılarak "Kazaa" programında sadece resim dosyaları üzerinde arama yapıldığında, arama sonucunda verilen 1.286 öğenin yaklaşık % 42'sinin çocuk pornografisi
resimleriyle bağlantılı olduğu tespit edilmiştir. En az 25 milyon çocuk internet kullanmaktadır. İnternet kullanan her dört çocuktan biri mutlaka sakıncalı sitelere girmekte ve yine her beş çocuktan biri de erişkinler tarafından cinsel tacize uğramaktadır. Sanal pedofili (küçük cocuklara cinsel ilgi duyma, cinsel ilişkiye girme) piyasası 5 milyon dolar, Unicef' in açıklamasına göre; ABD hariç çocuk pornografisinden elde edilen haksız kazanç 2–3 milyar dolardır. Çocuk şiddetini yansıtan fotoğrafların tanesi 30–200 dolara alıcı bulmaktadır. 1996 yılında ABD'de yapılan bir operasyon çerçevesinde 7 yaşına kadar Meksikalı çocuklar kullanılarak filmler çeken bir firmanın o zamanın parası ile 0,5 milyon dolar kazanç elde ettiği belirlenmiştir. Bu da bu piyasanın ne kadar büyük bir hacme sahip olduğunun bir göstergesidir. Dünya çapında yapılan operasyonlarda, bu suç icin alet edilen çocuk yaşınınn 3 aylık bebeğe kadar düştüğü ortaya çıkmıştır. Çocukların istismar edildiği porno siteleri sayısı 2002–2003 yılları arasında 200.000 kadardır. Bu sitelerin yarısından fazlası, ABD'de bulunuyor. En hızlı artış ise Rusya'da gözlemleniyor. Bütün bu göstergeler yanında mücadele icin calışmalar çok da başarılı olmamaktadır. Çünkü her ülkenin suça yönelik tanımlamasının farklı olması sonucu yaptıkları kanunlar da farklıdır. Dolayısıyla birlik sağlanamamakta bu da mücadelede sıkıntı yaratmaktadır… Çocuk pornosuna yönelik web sitelerinin sunucularının yurt dışı bağlantılı olması ve kendileri hakkındaki bilgilerin sahte düzenlenmesi Türkiye açısından çalışmaları daha da zorlaştırmaktadır. Ülkemizde sokakta yaşayan çok fazla çocuk olması da çocuk tacirlerinin iştahını kabartmakta, sorunlara başka bir boyut kazandırmaktadır…" bkz. Civiloğlu ve Tanyeri, a.g.e., s. 98, 99.

"yetkisiz erişim" düzenlenmiş olup suçun oluşumu için "bilgisayarın herhangi bir işlevinin yürütülmesine neden olma" oluşturmaktadır.[836] Anglo Amerikan hukuk sistemindeki teşebbüs müessesesi ile hukukumuzda yer alan teşebbüs müessesesi arasında farklılıklar bulunmakta olup İngiliz hukukunda TCK' dan farklı olarak teşebbüs ve bazen hazırlık hareketi sayılabilecek hareketler suçun içerisinde kabul edilerek tamamlanmış suç gibi cezalandırılabilmektedir.[837] Kanun' un 2. m.' sinde ise yetkisiz erişim suçunun başka suçların işlenmesini kolaylaştırmak veya sağlamak için işlenmesi ayrı bir suç olarak düzenlemiş AKSS' de sözleşmeye taraf ülkelere "bilgisayar verisi elde etme kastı ya da diğer dürüst olmayan kast" şeklinde suça ek kasıt aranabilme seçeneği sunulduğundan 2. m.' de de yetkisiz erişim hareketiyle diğer eklenen amaçlar arasında bağlantı kurulması suretiyle düzenleme yapılmıştır.[838] Bunun dışında 3. m. "Çeşitli yetkisiz eylemler" kısmında sistemin işleyişini bozmak, program veya verilere erişimi engellemek veya bunları gizlemek, veri güvenilirliğini bozma bu eylemleri, "Ciddi zarar riski oluşturan veya neden olan yetkisiz eylemler" (3ZA) kısmında ise bir önceki kısımda yer alan fiillerin ciddi zarar verme riski cezalandırılmakta, zarar verilebilecek alanlar, "insan refahı"[839], çevre, herhangi bir ülke ekonomisi veya ulusal güvenliği olmak üzere dört başlıkta belirlenmektedir.[840] Son olarak belirtelim ki 3A m.' sinde ise "1. ve 3. m.' lerde yer alan suçların işlenmesinde kullanılan araçların sağlanması veya elde edilmesi suçu" düzenlenmiş olup buna göre m. 1 veya 3'te tanımlanan bir suçu işlemek ya da işlenmesine yardımcı olmak kastıyla herhangi bir aracı yapan, uyarlayan, sağlayan veya sağlamayı teklif

836 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 205.
"Bu suçun oluşturulmasının arkasındaki düşünce, aslında bilişim korsanlarının yüzüne tüm kapıların kapanmasıdır. Bilişim korsanının kötü bir amacı olmasa da suç oluşur." Bkz. A.e.
"Erişimin hangi hallerde yetkisiz olacağı CMA'nın 17(5) maddesinde tanımlanmıştır. Buna göre "(i) Failin söz konusu yazılım ya da veriye erişim için yetkilendirilmiş bir kişi tarafından bir şekilde rıza gösterilmemiş olması" hallerinde veriye erişmesi durumunda yetkisiz erişim vardır." Bkz. A.e., s. 208.
837 A.e., s. 209.
838 A.e.
Etkin bir ceza kanununun hangi fiillerin suç işlemeyi kolaylaştırıcı suçlar olarak kabul edileceğinin belirlenmesini gerektirdiği, bunların bir suçlunun soruşturulmasını ve failin daha ağır suçlardan suçlanmasını sağlayan suçlar olduğu ancak bunların genellikle temel veya öne çıkan suçlar olarak kullanılmadığı, kanunun 1. ve 2. maddelerinde bulunan suçların bir çeşit "kolaylaştırıcı suçlar" olarak tanımlanabileceği belirtilmektedir. Bkz. A.e., s. 212.
839 "İnsan refahına verilen zararlar ise hayat kaybı, hastalık veya yaralanma, yiyecek, içecek veya enerji kaynaklarının bozulması, iletişim veya ulaşım imkanlarının bozulması veya sağlık servislerinin bozulması olarak sınırlı sayıda belirlenmiştir." Bkz. Karagöz, a.g.e., s. 103.
840 A.e.
Suç neticesinde yaşam kaybı, hastalık veya yaralanma ile ulusal güvenliğe yönelik bir zararın meydana gelmesi hali ise cezayı ağırlaştıran bir neden olarak kabul edilmiştir. Bkz. A.e.

eden bu suçu işlemiş olmaktadır.[841] Bunun yanında, sahtekarlık suçunda belirli bir aracın yapılması için özellikle dizayn edilen "makine, alet, belge ya da herhanhi bir materyalin" yapılması, bulundurulması ya da kontrol altında bulundurulması bunun yanında dolandırıcılık suçu açısından da dolandırıcılık eyleminde kullanılmak üzere bir aracın taşınması veya tedarik edilmesi suç olarak düzenlenmiştir.[842]

2.2.6. Rusya

Rusya' nın, 1998 yılından itibaren bilişim suçları ile ilgili m. ve düzenlemeleri Ceza Kanunu' na eklemiş olup "bilişim sistemleri kullanılarak her türlü pornografik materyalin üretimi ve dağıtımı (242.m)"[843], verilere ve yazılımlara hukuka aykırı etkide bulunma (272.m), veri ve yazılımlara zarar verecek yazılımların üretilmesi ve yayınlanması (273.m), bilişim sistemlerine ilişkin kuralların ihlali (m274), 152. m.' sinde çocuk ticareti ve kaçırılması fiilleri suç olarak düzenlenmiştir.[844]

G-8 ülkelerinin 1997 yılında Washington'da yaptıkları Adalet ve İçişleri Bakanları toplantısında kabul edilen bildiri ile "Ulusal Temas Noktaları" oluşturulmasına karar verilmesinden sonra İçişleri Bakanlığı bünyesinde ulusal temas noktası oluşturulmuş olup 24 saat kesintisiz çalışan bu bölüm ülke içindeki güvenlik ve yargı organlarının diğer ülkelerdeki eşdeğer organlarla doğrudan temas halinde bulunmaktadır.[845]

Rusya'nın bilişim suçlarıyla mücadelede çeşitli milletlere ait özel servislerin sınır ötesi erişimine ilişkin mevcut düzenlemesinden dolayı AKSS' yi imzalamayı reddettiği, bağlayıcı uluslararası sözleşmelere de kuşkuyla yaklaştığı belirtilmektedir.[846]

---

841 Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", s. 227.
"Bu suç tipi, 2006 tarihli Dolandırıcılık Yasası' nın (Fraud Act 2006) bilişim suçlarına son derece benzer bir yansımasını oluşturur. Normal şartlarda suçun oluşması için gerekli olan manevi unsur kasttır." Bkz. A.e.
842 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 455.
843 "242. maddesi Çocuk-Yetişkin ayrımı yapmadan ve internet ile bilgisayarı da kapsar tarzda genel ifadelerle kanuna aykırı pornografik materyalin çoğaltılması ve üretimi cezalandırılmaktadır." Bkz. Nacar, a.g.e., s. 36.
844 Eryaman, a.g.e., s. 48.
845 Nacar, a.g.e., s. 36; Eryaman, a.g.e., s. 48.
846 Eryaman, a.g.e., s. 49.

2.2.7. Japonya

Japonya' da mevcut gelişmiş teknoloji beraberinde bu alanda oluşabilecek suçlara (bilişim suçlarına) karşı önlem almada erken farkındalığın oluşmasını da sağlamıştır. Nitekim, 1987 yılında Ceza Hukuku Alanında Bazı Hükümler Değişiklik Yapılmasına İlişkin Kanun'la Japon Ceza Kanunu'na bilişim suçlarına ilişkin suç tiplerini dahil edilmiş[847], 13.02.2000 tarihinde ise "İnternete Haksız Girmenin Yasaklanması Hakkındaki Kanun" yürürlüğe girmiştir.[848] Salt bilişim suçları ise 03.02.2000 tarihinde yürürlüğe giren "Bilgisayarlara Yetkisiz Giriş Kanunu" nda düzenlenmiş olup 3. m.' de bilgisayarlara yetkisiz erişim; sınırlı şekilde erişimde bulunan ve şifre ile erişim sağlanan bilgisayara telekomünikasyon ağı üzerinden başka bir kişinin bilgileri aracılığıyla girilmesi, sınırlı şekilde erişimde bulunan bilgisayara telekomünikasyon ağı üzerinden, giriş önlemlerinden sıyrılacak tedbirleri uygulayarak erişim sağlanması ve başka bir bilgisayar ile kontrol edilen ve girişi sınırlı bulunan bilgisayara telekomünikasyon ağı üzerinden sistemin yetkisiz olarak erişilebilir hale getirilmesi olarak belirleniştir.[849] Yine aynı Kanun' da başka bir kişinin hakları, görevleri veya durumunun belgelendirilmesi ile ilgili izinsiz olarak elektromanyetik kayıt oluşturma, yetkisiz olarak başkasının finansal durumunu uygunsuz yönetmek amacıyla ödeme aracı olarak kredi kartı veya başka bir kart yapma, bu şekilde üretilen kartları bahsedilen amaçla bulundurma, bahsedilen kartlara ilişkin bilgileri edinme, iş için kullanılan bilgisayarlara zarar veren veya bilgisayar veya elektronik kayıtlarla yanlış veri veya sahte komut girişi gibi her türlü yolla ticaretin engellenmesine neden olma, dolandırıcılık suçları kapsamında, sahte elektromanyetik kayıt, sahte veri veya yetkisiz komutların üretilmesi veya kullanılmasıyla mülkiyet hakkının edinilmesi, kaybı veya değişikliğine neden olma, resmi makamlarca veya özel amaçlarla kullanılan bir belge veya elektromanyetik kayda zarar verme fiilleri suç olarak düzenlenmiştir.[850]

847 Eryaman, a.g.e., s. 46.
848 Nacar, a.g.e., s. 36.
849 Karagöz, a.g.e., s. 100-102.
850 A.e., s. 100-101.

BÖLÜM III

5237 SAYILI TÜRK CEZA KANUNUNDA BİLİŞİM ALANINDA SUÇLAR

3.1. GENEL OLARAK

Ceza mevzuatımıza bakıldığında, bilişim alanında suçların ilk kez 6 Haziran 1991 tarihli ve 3756 sayılı Kanun'un 20. m.' siyle 1 Mart 1926 tarihli ve 765 sayılı eski TCK' ya (11. Babta toplu olarak) Fransız Ceza Kanunu Projesinden yararlanılmak suretiyle[851] eklenen 525/a, 525/b, 525/c ve 525/d m.' leri ile gerçekleştiği görülmektedir.[852]

765 sayılı TCK' nın "Bilişim Alanında Suçlar" başlıklı 11. Babında:

"Madde 525/a- *Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve birmilyon liradan onbeşmilyon liraya kadar ağır para cezası verilir.*

Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir.

Madde 525/b- *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*

---

851 "Bilişim suçlarının 765 Sayılı TCK'de düzenlenmesinde ise, genel olarak 1989 tarihli Türk Ceza Kanunu Tasarısı esas alınmış olup, bu tasarıda yer alan hükümlerde ise Yeni Fransız Ceza Kanununun Öntasarısının 323-1 – 323-7 maddelerinde yer alan -88-19 no.lu Kanun ile eklenen 462-2 – 462-9 maddelerinin model alındığı- hükümlerden esinlenilmiştir." Bkz. Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları,* s. 59.

'…TCKT'deki hükümlerin tertibinde YFCK Ön Tasarısı'ndaki 321-1 -323-7 maddelerinden esinlenilmiştir.' Bkz. Sulhi Dönmezer, Kişilere ve Mala Karşı Cürümler, Beta Basım Yayım Dağıtım, İstanbul, 2001, s. 613 (*Aktaran* Eker, a.g.e., s. 111).

"Ancak bu suçlar Fransız Ceza Kanununda olduğu gibi "Mal Aleyhinde İşlenen Suçlar" bölümünde hüküm altına alınmamış, Türk Ceza Kanunun "Cürümler" başlığını taşıyan ikinci kitabının, "Bilişim Alanında Suçlar" adını taşıyan ikinci kitabının, "Bilişim Alanında Suçlar" adını taşıyan onbirinci babında düzenlenmiştir." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 97.

852 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 58; Akbulut, *Bilişim Alanında Suçlar*, s. 96; Eker, a.g.e., s. 111.

değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beşmilyon liradan ellimilyon liraya kadar ağır para cezası verilir.

Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmimilyon liraya kadar ağır para cezası verilir.

Madde 525/c- *Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrif eden kimseye bir yıldan üç yıla kadar, tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir."*[853]

765 sayılı TCK' da gerçekleştirilen bu değişikliğin sonucunda, kanunun kabul etmiş olduğu hukuki değer esası göz önünde bulundurulmadan bilişim suçlarının ayrı bir babda düzenlenmesinin TCK sistematiğine aykırı olduğu[854], düzenlenen hükümlerin yetersiz olduğu, hükümlerde kullanılan "bilgileri otomatik işleme tâbi tutmuş sistem" ifadesinin yerinde bir seçim olmadığı, hükümlerin taksirli şeklinin düzenlenmediği, hükümlerin genel olarak düzenlenmesinin kanunilik ve belirlilik ilkeleri açısından sorun oluşturduğu gibi getirilen eleştiriler yanında yapılan düzenlemelerin dönemine göre ileri bir sistem getirdiği, bilgisayar yerine "bilgileri otomatik işleme tâbi tutmuş sistem" ifadesinin doğru bir tercih olduğu, suçların ayrı bir babda düzenlenmesinin uygulama kolaylığı getirdiği[855] gibi görüşler de ileri sürülmüştür.[856]

853 Şahin ve Özgenç, a.g.e., s. 513.

854 "…Sistematik olarak incelendiğinde, bilişim alanında suçların düzenlenmesinde, bu suçların hukuki konularına ve söz konusu hukuki konular arasında yapılan tercihe göre düzenlenmesi şeklindeki, Alman ve İtalyan Ceza Kanunlarına hakim olan yaklaşımın, 765 sayılı TCK'de olduğu gibi 5237 Sayılı TCK'de de tercih edilmediği görülmektedir.

Bu açıdan, tercih edilen sistem, yürürlükteki Fransız Ceza Kanununun 323 vd. maddelerinde olduğu gibi bu suçların bir arada düzenlenmesi şeklindedir. Buna karşın, söz konusu suçlar, Fransız Ceza Kanununda, kişilere karşı suçlar arasında malvarlığına karşı diğer suçlar başlığı altında düzenlenmiş olup, bu haliyle hukuki konu bakımından bir tercihin sonucunu yansıttığı görülebilmektedir. Bu doğrultuda, bilişim alanında suçların 5237 Sayılı TCK'de"Topluma Karşı Suçlar" arasında düzenlenmesi nedeniyle, TCK'nin, bilişim alanında suçlar bakımından sistematiği Fransız Ceza Kanunundaki sistematikten de farklılık göstermektedir." Bkz. Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 62.

855 Demircan' a göre: "Bilişim alanında suçları korunan hukuki yarar gözetilmek suretiyle ceza kanununda ilgili suç tiplerinin altına yerleştirmek yerine, ayrı bir bölümde toplamak, uygulamacıya da kolaylık sağlaması açısından yerinde olmuştur. Ayrıca bilişim alanına ilişkin özel bir kanun yapılması yerine, bu şekilde mevcut düzenlemelerin bilişim alanını ilgilendirecek kısımlarında değişiklikler yapılması gereken noktalarda yeni düzenlemeler yapılarak yeni suç tiplerinin getirilmesi yerinde olmuştur." Bkz. Demircan, a.g.e., s. 64.

856 Ayrıntılı bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 102-105.

5237 sayılı yeni TCK' da ise ikinci Kitabın "Topluma Karşı Suçlar" başlıklı üçüncü kısmının "Bilişim Alanında Suçlar"[857] başlıklı 10. Bölümünde, 243. m. : "Bilişim Sistemine Girme", 244. m. : "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", 245. m. : "Banka veya Kredi Kartlarının Kötüye Kullanılması" ve 245/A m. : "Yasak Cihaz veya Programlar" suç tiplerini düzenlemiştir.[858] Türk Ceza Hukukunda bilişim alanında suçlar bakımından özel bir kanun yerine Türk Ceza Kanunu' nda düzenleme tercihinin yapıldığı, hem 765 sayılı TCK' da hem de 5237 sayılı TCK'da suçların hukuki konusu bakımından yeterli inceleme yapılmaksızın uygulamada kolaylık sağlamak üzere ayrı bir bölümde ve topluca düzenlenmiş olduğunu belirten yazarlar bulunmaktadır.[859] Yeni TCK' da bilişim suçları düzenlenirken karma yöntem tercih edilerek hem yeni hükümler eklenmiş hem de geleneksel suç tiplerinin işleniş biçimleri çeşitlendirilerek yeni suç tipleri eklenmiştir.[860] Nitelikli hırsızlık (m. 142), nitelikli dolandırıcılık (m. 158), kumar oynanması için yer ve imkân sağlama (m. 228) suçlarında olduğu gibi bilişim sistemlerinin kullanılmasının nitelikli hal olarak düzenlendiği suç tiplerinin yanında haberleşmenin engellenmesi suçu (124. m.), hakaret suçu (125. m.), kişisel verilerin ele geçirilmesi (136. m.), kişisel verilerin kaydedilmesi (135. m.) gibi doğrudan bilişim sisteminden bahsedilmemiş olsa dahi eylemin bilişim sistemleri kullanılarak

857 "Bu bölüm başlığı, TBMM Adalet Komisyonunda "Bilişim Sistemlerine Karşı Suçlar" olarak kabul edilmişti. Ancak, TBMM Genel Kurulunda verilen bir önerge üzerine, Bölüm başlığı, Hükümet Tasarısında olduğu gibi, "Bilişim Alanında Suçlar" olarak değiştirilmiştir." Bkz. Şahin ve Özgenç, a.g.e., s. 321.

858 Demircan, a.g.e., s. 64; Akbulut, *Bilişim Alanında Suçlar*, s. 105.
"5237 sayılı Türk Ceza Kanunu bilişim suçlarını "Bilişim Alanında Suçlar" başlığı altında düzenlemekle yetinmemiş, bilişim sistemlerinin araç olarak kullanıldığı suçlara çeşitli başlıklar altında da yeni suç tiplerine yer vermiştir." Bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 210.

859 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 65, 66.

860 Demircan, a.g.e., s. 65.
"TCK iki kitap halinde hazırlanmış, kitaplar kısımlara, kısımlar da bölümlere ayrılmıştır. İlk kitapta yine 765 sayılı ETCK'da olduğu gibi ceza hukukunun genel ilkeleri belirtilmiş ve bu kitap üç kısma ayrılmıştır. İkinci kitap ise "insanlığa karşı suçlar", "kişilere karşı suçlar", "topluma karşı suçlar" ve "millete ve devlete karşı suçlar ve son hükümler" şeklinde dört kısma ayrılmış ve bu ayrıma göre suç tipleri düzenlenmiştir.
Bunlardan "kişilere karşı suçlar" kısmının dokuzuncu bölümünde "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında ve "topluma karşı suçlar" kısmının onuncu bölümünde "bilişim alanında suçlar" başlığı altında bazı bilişim suçu tipleri düzenlenmiştir. Bunların yanı sıra bilişim sistemi aracılığıyla işlenebilecek, "kişilere karşı suçlar" kısmının yedinci bölümü olan "hürriyete karşı suçlar" bölümünde "haberleşmenin engellenmesi suçu", sekizinci bölüm olan "şerefe karşı suçlar" bölümünde "hakaret suçu", malvarlığına karşı suçlar bölümünde "nitelikli hırsızlık suçu" ve "nitelikli dolandırıcılık suçu" ile "topluma karşı suçlar" kısmının yedinci bölümü olan "genel ahlaka karşı suçlar" bölümünde "müstehcenlik suçu" da düzenlenmiştir. Son olarak yine genel ahlaka karşı suçlar bölümünün altında yer alan "kumar oynanması için yer ve imkan sağlama" suçu, 15.08.2017 tarihli 694 sayılı KHK ile yapılan değişiklikle bilişim sistemleri aracılığıyla işlenebilecek suçlar arasına girmiştir." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 228.

işlenebileceği suç tipleri de mevcuttur.[861] Ancak Akbulut' a göre farklı hukuki değerleri koruyan suçların aynı bölümde düzenlenmesi mağdurun kim olduğu, korunan hukuki değerin ne olduğu gibi hususlarda tartışmalara neden olabilecek ve esasen TCK sistemimize göre korunan hukuki değere göre suçların ilgili bölümlere yerleştirilmesi gerekmektedir.[862]

5237 sayılı TCK' da 243. m. ile ilk kez bir bilişim sistemine hukuka aykırı girme suç olarak düzenlenmiş[863], 765 sayılı TCK' da 525/b-1' de tek suç içerisinde yer alan verilere veya sisteme müdahale niteliği taşıyan eylemler 5237 sayılı TCK' nın 244. m.' sinde ayrı ayrı suçlar olarak düzenlenmiş ve 525/b-2' de düzenlenen bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak yarar sağlama suçu ise yeni TCK' da 244. m.' nin 4. fıkrasında belirli hareketlerin gerçekleştirilmesi koşulu ile suç olarak öngörülmüştür.[864] 765 sayılı TCK' nın 525/c m.' sinde "Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak

861 Karagöz, a.g.e., s. 108.

862 Ayrıntılı bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 108.

863 Demircan, a.g.e., s. 65.

5237 sayılı T.C.K.'nın 243. maddesinin 765 sayılı TCK.'nın 525a maddesine denk geldiği belirtilmekte ise de 243. maddede, 525a maddesindeki gibi ele geçirme suçu bulunmamaktadır. Dolayısıyla verilerin ele geçirilmesi şartı aranmaksızın bilişim sistemine girilmesi başlı başına bir suç olarak düzenlenmiş bulunmaktadır. Bkz. Uçar, a.g.e., s. 47.

"ETCK'nın 525a/1. maddesinde "verilerin ele geçirilmesi" suçu düzenlenmiş, bilişim sisteminin güvenliğinin kırılarak sisteme hukuka aykırı olarak girilmesi ve orada kalınması eylemleri ise suç olarak tanımlanmamıştı." Bkz. Ali Parlar ve Muzaffer Hatipoğlu, *Açıklamalı – Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu (230 – 345 Maddeler)*, 4. Cilt, Seçkin Yayınevi, Ankara, 2010, s. 3741.

"TCK'nın 243'üncü maddesinde düzenlenen bilişim sistemine girmek ve orada kalmaya devam etmek suçu, 765 S. TCK'nın 525a/1 ve 525a/2 de yer alan "verilerin ele geçirilmesi" ve "ele geçirilen verilerin zarar vermek üzere kullanılmaları" suçlarının karşılığı olarak düzenlenmiş gibi görünse de, bu suçları düzenlememektedir. Böylece artık verilerin ele geçirilmesi hatta elde edilen verilerin kullanılmaları bazı durumlarda yaptırımsız kalmaktadır. Bununla beraber ele geçirilen veriler kişisel nitelikte ise, kişisel verilerin hukuka aykırı olarak ele geçirilmesini yaptırım altına alan Kanun'un 136'ncı maddesi, veriler sistemden kaldırılarak ele geçirilecek olursa bu sefer 244(2)'nci maddesi gündeme gelebilecektir. Ancak sistemden kopyalanan veriler her zaman kişisel veri niteliğinde olamayacağı gibi, birçok kez kopyalanarak elde edildikleri için de sistemden kaldırılması söz konusu olmayacaktır." Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, s. 110.

864 Akbulut, *Bilişim Alanında Suçlar*, s. 107.

"…525b maddesindeki hükme baktığımızda burada amacın doğrudan bilişim sistemini korumak olmadığı; yarar sağlamak maksadıyla bilişim sistemine yapılan müdahalelerin cezalandırıldığı görülmektedir. Buna karşılık 244'üncü maddedeki düzenlemenin özellikle ilk üç fıkrası, doğrudan bilişim sistemini ve bu sistemdeki verileri korumaya yöneliktir. Bir başka deyişle, eski kanunumuz bilişim sistemine veya verilere zarar vermeye yönelik fiilleri, failin yarar sağlamak maksadıyla hareket etmesi halinde cezalandırırken; yeni kanunumuz bu tür saldırıları cezalandırmak için yarar sağlamak maksadına bir manevi unsur olarak yer vermemektedir. Bununla birlikte 244'üncü maddenin 4'üncü fıkrasında düzenlenen bilişim sistemini kullanarak haksız yarar sağlamak suçu ile bu suçun karşılığını oluşturan 525b maddesinin 2'nci fıkrasındaki düzenleme büyük ölçüde paralellik taşımaktadır." Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 112.

işleme tabi tutma bir sisteme, verileri veya diğer unsurları yerleştirme veya var olan verileri, diğer unsurları tahrif etme"[865] şeklinde suç olarak düzenlenen verilerde sahtecilik hükmüne ise yeni TCK' da yer verilmemiştir.[866] Kanaatimizce de bu bir eksiklik oluşturmaktadır. Bunun yanında, 765 sayılı TCK'da yer alan 525a/2 m.' sinde düzenlenen "bilgileri otomatik isleme tabi tutmuş bir sistemde yer alan bir program, veri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanma, nakletme veya çoğaltma" suçu da 5237 sayılı TCK' da yer almamaktadır.[867] 24 Mart 2016 tarihli ve 6698 sayılı Kanunla, 5237 sayılı TCK' nın 243. m.' sinde yer alan "ve" bağlacı "veya" olarak değiştirilmiş bunun yanında maddeye dördüncü fıkra olarak "veri nakillerini teknik araçlarla izleme suçu" eklenerek AKSS' nin ilgili hükümlerine paralel bir düzenlemeler gerçekleştirilmiştir.[868]

5237 sayılı TCK ile 765 sayılı TCK' da olduğu gibi ayrı bir bölüm altında toplu şekilde bilişim alanında suçların düzenlenmesinde suçların hukuki konusunda ortaya çıkan sistematiğe ilişkin tartışma yeni boyut kazandığı bu yeni tartışmanın, bilişim alanında suçların topluma karşı suçlar arasında düzenlenmesini gerektirecek topluma ait bir yararın korunmasına yönelik olup olmadığı, bu sorunun yansımasının ise bilişim alanında işlenen suçlar için TCK' da genel hukuka uygunluk sebebi olan ilgilinin rızası hükümlerinin uygulanıp uygulanamayacağı hususlarında karşımıza çıktığı belirtilmektedir.[869] Bu bağlamda, Değirmenci gibi, bilişim alanında suçların mevcut düzenleme yerinin uygun olduğunu savunan yazarlar olduğu gibi Ketizmen gibi aksi görüşte olan yazarlar da bulunmaktadır. Değirmenci' ye göre bilişim sistemlerine karşı veya bilişim sistemleri aracılığıyla işlenen suçların kişilerin hak ve menfaatlerini ihlal

865 Uçar, a.g.e., s. 45.

866 Akbulut' un da belirtmiş olduğu üzere Elektronik İmza Kanunu' nun 17. maddesinde yer alan elektronik sertifikalarda sahtekarlık eyleminin suç olarak yer aldığı düzenleme tüm verileri kapsamadığından bunun yanında 245. maddenin 2. fıkrasında banka ve kredi kartlarında sahtecilik düzenlemesi de sadece banka veya kredi kartı üretmeyi cezalandırdığından bu hükme yer verilmemesi mevzuatımızda bir eksiklik oluşturmaktadır. Ayrıntılı bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 106.

"…TCK düzenlenirken AKSSS'de taraf devletlere, 7'inci maddeyle, yüklenen "bilgisayarla ilişkili sahtecilik eylemlerinin" yaptırım altına alınmasına ilişkin düzenleme göz ardı edilmiş durumdadır. Kanun, günümüzde resmi veya özel kurum ve oluşumların artık nerede ise tamamıyla bilgisayarlar marifetiyle belge hazırladıklarını dikkate almayarak bu nevi belgelerde yapılan eylemler sonucu resmi veya özel evrakta sahtecilik suçu söz konusu olması gerekecekken, faillerin verileri değiştirme veya yok etme suçuyla ödüllendirilmesi söz konusu olacaktır. Diğer bir deyişle, resmi evrakta sahtekarlığı bilişim sisteminde manipülasyonlar yapmak suretiyle elde etmek, bu fiil için öngörülen ceza miktarı göz önüne alındığında fail bakımından daha avantajlı olacaktır." Bkz. Erdoğan, Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle), s. 114.

867 Uçar, a.g.e., s. 48.

868 Bkz. Koca ve Üzülmez, a.g.e, s. 804.

869 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 62.

etme olasılığı mevcut ise de bu suçların aracı edilmesi suretiyle toplumun ve menfaatlerinin ihlal edilmesi ihtimalinin diğer olasılıktan önce düşünülmesi gerekmekte olup başka bir anlatımla Değirmenci tarafından bilişim suçları aracılığı ile ihlal edilen hak ve menfaatlerden topluma ait olanların daha önemli olması sebebiyle "Bilişim Alanında Suçlar" ın düzenleme yerinin uygun olduğu belirtilmektedir.[870] Ketizmen' e göre ise, bilişim sistemlerinin toplumsal zarara yol açabileceği hususunda doğru bir noktaya değinilmekte ise de TCK' nın genel gerekçesinde bilişim alanında suçlar başlığı altında düzenlenen suçların topluma zarar verebilecek nitelikte olup olmadığına ilişkin herhangi bir açıklamaya yer verilmemiş olunması, banka ve kredi kartlarının kötüye kullanılması suçunun düzenlendiği 245. m.' nin gerekçesinde ise bu maddede düzenlenen fiillerin kişiye ait hukuki yararları korumaya yönelik olduğunun açıkça belirtilmesi, 244. m.' nin birinci ve ikinci fıkralarında düzenlenen fiiller bakımından suçun toplumsal bir yarardan ziyade kişiye ait bir yararı koruması, yine 244. m.' nin son fıkrasında yer alan, 244. m.' de belirtilen fiillerin işlenmesi suretiyle yarar sağlamaya ilişkin düzenlemenin gerekçesinde malvarlığına ilişkin bir değerin saldırıya uğramasına ve ihlal edilmesine vurgu yapılması hususlarının birlikte değerlendirilmesi sonucunda, bilişim alanında işlenen suçların Türk Ceza Hukuku sisteminde sağlıklı bir yer edinebilmesi ve uygulanabilmesi bakımından, bilişim alanında suçların hukuki konusu ve yorumunda, Kanunun sistematiğinin esas alınması

870 Değirmenci, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", s. 198, 199.
Dülger ise: "Söz konusu düzenlemede, bilişim suçları açısından 765 sayılı ETCK için en yoğun eleştirilerin yapıldığı sistematik değiştirilmiş; bilişim suçları, suçla korunan hukuksal değer gözetilerek düzenlenmiş, suç tipleri arasında bunların korudukları hukuksal değerin niteliğine göre ayrım yapılmıştır; ancak "banka ve kredi kartlarının kullanılması suçu" açısından bu ayrım yapılmayarak, bu suçun koruduğu hukuksal değer göz önüne alınmaksızın bilişim sistemlerine karşı suçlar bölümünde düzenlenmiştir. Buna bağlı olarak daha sonra eklenen suç tiplerine de (m. 243/4 ve 245/A gibi) bu bölüm içerisinde yer verilmiştir.
…Modern ceza hukuku öğretisinin merkez kavramını "suçla korunan hukuksal değer" oluşturur ve buna ceza hukukunda çeşitli işlevler yüklenir. Bunlar, hukuksal değerin "eleştiri", "suç politikası", "ceza normlarının meşruluğu", "suçları gruplandırma", "ceza yaptırımını gerekçelendirme, sınıflandırma ve denetleme" ve "yorum aracı olma" işlevleridir. İşte ben de hem suç teorisini algılayışımda hem de kitabımın konusu olan bilişim suçlarına ilişkin açıklamalarımda suçla korunan hukuksal değer kavramını merkez olarak almakta ve yukarıda belirtilen işlevleri dikkate almak suretiyle bilişim suçlarıyla ilgili ortaya çıkan kuramsal sorunları bu kavram ve suç teorisinin önermeleri doğrultusunda çözmeye çalışmaktayım." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 228, 229, 233.
"…5237 sayılı TCK'da bu durum göz önüne alınarak düzenleme yapılmaya çalışılmış ve bilişim suçları mümkün olduğunca koruduğu hukuksal değere göre ilgili olduğu bölümlerde düzenlenmiş, belli bir bölüme sokulmayan ya da korudukları hukuksal değer özellikle bilişim sisteminden elde edilen yararla birebir bağlantılı olan ya da aynı anda birden fazla hukuksal değeri koruyan suç tipleri "bilişim alanında suçlar" başlığında ayrı bir bölümde düzenlenmiştir." Bkz. A.e., s. 243.

yerine her maddede düzenlenen normun kendisinin esas alınması önem arz etmektedir.[871]

Soyaslan' ın da belirtmiş olduğu üzere, TCK' da yer alan özel hükümler bölümü suçun hukuki konusuna göre kısımlara bölünmüşse de kısımları oluşturan bölümler ise failin sıfatı, hareketin yapısı, fiilin konusu, kullanılan vasıta, zaman ve yer gibi suçun maddi ve manevi unsurlarına dayanılarak maddeleştirilmiştir.[872] Bu bağlamda kanaatimizce günümüz hayatının vazgeçilmez unsuru haline gelen ve toplumun büyük bir kısmının hatta kamu kurum ve kuruluşlarının da önemli iş ve işlemlerinde kullanılan bilgi teknolojileri ve bilişim sistemleri ile işlenen suçların bireylerin menfaatinden ziyade tüm toplumu etkileyebilecek nitelikte olması, bu sistemlerin güvenliğinin tüm toplumun menfaatlerini koruma açısından önem arz etmesi sebepleriyle bilişim alanında işlenen suçların topluma karşı suçlar kısmında düzenlenmesi yerinde bir düzenleme olarak görülmektedir. Nitekim, çalışmamız içerisinde belirtmiş olduğumuz üzere kritik altyapı hizmetlerinin tüm topluma hizmet etmesi ve bunlara gerçekleştirilen saldırıların tüm toplumun menfaatlerini etkileyecek olması sebebiyle bu durumun ayrıca değerlendirilerek "bilişim alanında suçlar" bölümünde yeni madde düzenlemesi de değerlendirilmelidir. Bunun yanında, Akbulut' un da belirtmiş olduğu gibi esasen TCK sistemimize göre korunan hukuki değere göre suçların ilgili bölümlere yerleştirilmesi gerekmekte[873] olup bu anlamda

871 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 64-67.
Yine Akbulut' a göre de: "…Oysa sistemimize göre korunan hukuki değere göre suçların ilgili bölümlere yerleştirilmesi gerekirdi. Ayrıca kanun koyucunun bazı suçların bilişim araçları aracılığıyla işlenebileceğini kabul ederek (hırsızlık, dolandırıcılık, kumar oynanması için yer ve imkân sağlanması gibi) ilgili bölümde yer vermesi, bilişim suçları niteliği taşıyan bazı suçları özel kanunlarda düzenlenmesi (Örneğin Elektronik İmza Kanunundaki elektronik sertifikalarda sahtekârlık fiili gibi) çoğunlukla bilişim araçlarının kullanılması suretiyle işlenecek bazı suçları korunan hukuki değere göre ilgili bölüme yerleştirmesi (kişisel verilerin ele geçirilmesi TCK m. 136, kişisel verilerin kaydedilmesi TCK m. 135), ancak m. 243 vd. maddelerinde düzenlenen suçlarda farklı tercihte bulunması bunun sorgulanması sonucunu doğurmaktadır. Farklı hukuki değerleri koruyan suçların aynı bölümde düzenlenmesi mağdurun kim olduğu, korunan hukuki değerin ne olduğu noktasında ileride de görüleceği gibi tartışmalara neden olmaktadır." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 108.
"Tüm bunların yanı sıra bilişim suçlarının geçirdiği evrim, günlük hayatın her alanında yaygın şekilde karşılaşılabilmesi göz önünde alındığında artık bilişim suçlarının "Topluma Karşı Suçlar" kısmı yerine "Kişilere Karşı Suçlar" kısmı içerisinde düzenlenmesi gerektiğini düşünmekteyiz. Suçtan kaynaklanan baskın zararın kişiler üzerinde oluşması ve TCK sistematiğinde "Kişilere Karşı Suçlar"a verilen önem nedeniyle, bilişim alanında suçlara da aynı önemin verildiğinin gösterilmesi amacıyla bu bölüm içerisinde yer alması uygun olacaktır. Nitekim TCK m. 245/5'e göre malvarlığı suçlarına ilişkin etkin pişmanlık hükümlerinin uygulanması, malvarlığına ilişkin suçların da "Kişilere Karşı Suçlar" kısmında düzenlenmesi, bilişim alanında suçların "Kişilere Karşı Suçlar"la olan yakın bağlantısını da ortaya koymaktadır." Bkz. Karagöz, a.g.e., s. 109.
872 Doğan Soyaslan, *Ceza Hukuku Özel Hükümler*, 11. Bsk., Yetkin Basımevi, Ankara, 2016, s. 70.
873 Ayrıntılı bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 108.

bilişim alanında suçlar bölümünde yer alan 243 ve 244. m.' lerinin korudukları hukuksal değer göz önüne alındığında da bu suçların bilişim alanında suçlar bölümünde düzenlenmesinde bir isabetsizlik görülmemektedir. Ancak 245. m.' de düzenlemesinin koruduğu hukuksal yarar diğer maddelerden farklı olduğu düşünüldüğünden bu madde açısından bir eleştiri getirilebileceğini düşünmekle beraber bu husus ilgili suç başlığı altında irdelenecektir.

3.2. 5237 SAYILI TCK' DA BİLİŞİM ALANINDA SUÇLAR

TCK'nın "Topluma Karşı Suçlar" başlığını taşıyan ikinci kitabının "Bilişim Alanında Suçlar" başlığını taşıyan Onuncu bölümünde yer alan 243. m. "*Bilişim Sistemine Girme*", 244. m. "*Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme*", 245. m. "*Banka veya Kredi Kartlarının Kötüye Kullanılması*" ve 245/A' da yer alan "*Yasak cihaz veya programlar"* suçları bu başlık altında incelenecektir.

3.2.1. Bilişim Sistemine Girme veya Sistemde Kalma Suçu (TCK madde 243/1)

5237 sayılı TCK' nın "Bilişim Sistemine Girme" başlıklı 243. m.' si:

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

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

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

(4) 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."[874] şeklinde düzenlenmiştir.[875]

874
https://mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch=t%C3%BCrk%20ceza&Tur=1&Tertip=5&No=5237, ET. 5 Mart 2020.

875 "GEREKÇE
Bilişim sistemlerine karşı suçların düzenlendiği Bölümde yer alan bu maddede bilişim sistemine girme fiili suç olarak tanımlanmıştır.
Bilişim sistemlerinden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.
Maddenin birinci fıkrasında bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiili suç hâline getirilmiştir. Siteme, hukuka aykırı olarak gihren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir.
İkinci fıkraya göre, birinci fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, bu suç açısından daha az ceza ile cezalandırılmayı gerektirmektedir.

Bilişim sistemlerine izinsiz giriş, "bilgisayara tecavüz", "kod kırma", "bilgisayar korsanlığı" olarak da ifade edilen[876] olan "bilişim sistemine girme suçu" nun karşılığı 765 sayılı TCK' da yer almamaktaydı.[877] 1997 tarihli TCK Tasarısının "347. m.' si"[878]nde bu suç tipi düzenlenerek hapis cezası ile adli para cezası öngörülmüş, 2000 Tasarısının "345. m.'si"[879]nde para cezası miktarı dışında madde aynen korunmuş, 2003 tarihli Tasarının "346. m.'si"[880]nde de sadece para cezasının miktarında değişiklik yapılmışken 243. m.'nin kanunlaşması sırasında Tasarılarda yer alan teşebbüsle ilgili hüküm metne alınmayarak sisteme girme veya orada kalma, sisteme girme ve orada kalma olarak değiştirilerek hükme bağlanmış, hapis cezası ile adlî para cezası ise seçimlik olarak öngörülerek yürürlüğe girmiştir.[881] Ancak maddenin birinci fıkrasında yer alan sisteme girmek ve orada kalmaya devam etmek ifadeleri arasındaki ve bağlacı 6698 sayılı Kanun' un 30. m.'si ile veya şeklinde değiştirilerek söz konusu suç, bağlı hareketli suçtan seçimlik hareketli suç haline getirilerek iç hukukumuzun bir parçası olan AKSS' deki ilgili hüküm ile paralel hale

---

Üçüncü fıkrada, bu suçun neticesi sebebiyle ağırlaşmış hâli düzenlenmiştir. Birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.

Sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır." Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7285; Şahin ve Özgenç, a.g.e., s. 321.

876 Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", Prof. Dr. Burhan Ceyhan'a Armağan II, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 12, Özel Sayı, Yıl: 2010, İzmir, 2012, ss. 1363-1432, s. 1365; Apaydın, "Bilişim Sistemine Girme Suçu", s. 253.

877 "765 sayılı TCK ile karşılaştırıldığında, 765 sayılı TCK nın 525/a maddesinin metnine 5237 sayılı Yasanın 243. maddesi bazı yönlerden benzemekte ise de; önceki kanunda bu maddenin tam karşılığı yoktur. 765 sayılı TCK'nın 525/a. maddesinde, verilerin ele geçirilmesi suç olarak düzenlenmişken, YTCK'nın 243. maddenin özellikle birinci fıkrası ile bilişim sistemine girme ve orada kalmaya devam etme eylemi suç olarak düzenlenmiş, bu girme sonucu sistemin içerdiği verilerin yok olması veya değişmesi durumu, üçüncü fıkra kapsamına alınmıştır." bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7286.

878 "347. madde: "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve yüzmilyon liradan üçyüzmilyon liraya kadar apğır para cezası verilir.

Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir." Bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 113, dipnot. 299.

879 "345. madde: "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve birmilyar liradan üçmilyar liraya kadar ağır para cezası verilir.

Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir." Bkz. A.e., s, 114, dipnot. 301.

880 "346. madde: "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve üçmilyar liradan onmilyar liraya kadar ağır para cezası verilir.

Bu fiil nedeniyle sistemin içerdiği veriler yok edilir ve değişirse faile iki yıldan dört yıla kadar hapis ve beşmilyar liradan onbeşmilyara liraya kadar ağır para cezası verilir.

Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir." Bkz. A.e., s, 114, dipnot. 302.

881 Bkz. A.e., s. 112-114.

getirilmiş ve değişiklik öncesinde doktrinde yer alan eleştiriler karşılanmıştır.[882] Burada belirmek gerekir ki, sadece ve başlı başına bilişim sistemine girmenin suç olarak düzenlenmiş olduğu 243. m. etkili ve yerinde olsa da tasarılarda yer aldığı hali ile teşebbüs halinde kalan hareketlerin de tamamlanmış suçtan cezalandırılması esasının benimsenmesinin eylemleri önlemede daha etkin sonuçlar doğuracağı ve suçla mücadelede daha etkili olacağını düşünmekteyiz.[883] Nitekim, Alman Ceza Kanunu' nda yer alan düzenlemelere bakıldığında da düzenlenen birçok suç tipide teşebbüs halinde kalan suçun cezalandırılacağına vurgu yapıldığı[884], bilgisayar sabotajının düzenlendiği 303b m.'sinde bunun yanında suça hazırlık hareketlerinin de 202c m. uyarınca cezalandırılacağı hükme bağlanmıştır. Nitekim, Dülger de bu suç tipi için sisteme yetkisiz giriş ve veri ele geçirmeyi sağlayan yazılımların üretilmesi ve yayılmasının suç haline getirilmesi gerektiği fikrini ileri sürerken Alman Ceza Kanunu' nun "Veri Casusluğunun ve Verilerin İletilirken Ele Geçirilmesinin Hazırlığı" başlıklı 202c m.'sini örnek olarak göstermiştir.[885]

882 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 236.
"TCK'nın 243. maddesinin ilk fıkrasının TBMM Adalet Komisyonunda kabul edilen şeklinde bilişim sistemine girme suçu "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden" şeklinde seçimlik hareketli bir suç olarak düzenlenmişti. Kanunun TBMM Genel Kurulunda yapılan görüşmeleri sırasında verilen bir önerge üzerine fıkra metnindeki "veya" bağlacı "ve" şeklinde değiştirilmiş ve bu şekilde kanunlaşmıştı. Bu değişiklikten hareketle doktrinde suçun oluşması için sisteme girmenin yeterli olmadığı ayrıca sistemde kalmaya devam edilmesi gerektiği, sisteme girmesine rağmen kalmadan çıkan kişinin fiilinin suç oluşturmayacağı söylenmişti. Hatta daha da ileri gidilerek TBMM Genel Kurulunda yapılan değişiklik nedeniyle Sözleşmenin 2. maddesinde suç olarak düzenlenmesi öngörülen bilişim sistemine yetkisiz erişimin ülkemiz hukuku açısından suç olmaktan çıktığı belirtilmişti. Bu düzenlemenin hatalı olduğunu ve yapılacak bir değişiklikle fıkradaki "ve" bağlacının "veya" haline getirilmesi gerektiğini kabul etmekle birlikte, yapılan bu değişikliğe fazla anlam yüklememek gerektiğini ve hükmü yorumlarken değişiklik gerekçesinin göz önünde tutulması gerektiğini savunmuştuk. 6698 sayılı Kanunla fıkradaki "ve" ibaresi "veya" şeklinde değiştirilerek, bütün bu tartışmalara son verilmiştir." Bkz. Koca ve Üzülmez, a.g.e., s. 807.
883 Aynı yönde görüş için bkz. Ali Karagülmez, "Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu", *Türkiye Adalet Akademisi Dergisi*, Cilt:1, Yıl:1, Sayı:3, Ekim 2010, ss. 235, 256, s. 255.
884 "Belçika Ceza Kanununun 550(b) maddesinin; (1) numaralı fıkrasındaki haksız erişimin işlenmeye teşebbüs edilmesi dahi tamamlanmış suç olarak kabul edilmiştir. Finlandiya Ceza Kanununda da bilişim sistemine zorla girme fiilinin teşebbüsünde benzer bir düzenleme yer almaktadır." Bkz. A.e.
885 "Ülkemizde de bu tür eylemlerle etkili bir mücadelenin yürütülebilmesi için benzer bir suç tipinin oluşturularak ceza yasasına alınması gerekir. Nitekim yasa koyucu bu ve benzeri eleştirileri dikkate alarak 6698 sayılı Yasanın 30. maddesiyle TCK'ya eklediği 245'A maddesiyle banka ve kredi kartlarının kötüye kullanılması suçları açısından hazırlık hareketi niteliğindeki yasak cihaz ve programlarla ilgili bir düzenleme yapmıştır. Ancak bu yalnızca banka veya kredi kartlarının kötüye kullanılması suçları açısından değil, diğer bilişim suçları açısından da geçerli olması gereken bir husustur." bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 238, 239.
Aynı yönde görüşe haiz olan Karagülmez' e göre de: "Yukarıda temas edildiği üzere, haksız erişimin suç sayıldığı bilişim sisteminin şifre ve sair güvenlik önlemiyle korunuyor olması, bilişim suçlarıyla mücadelede büyük önem taşımaktadır. Bunun doğal bir sonucu olarak da, bazı düzenlemelerde bilişim sistemlerindeki "şifre" ve benzeri "güvenlik yapıları"nın ele geçirilmesi ya da bunu sağlayan

Kanun koyucu, bilişim suçlarının çoğunun sisteme girilmek suretiyle başlaması ve sistem ve içerdiği verilerin güvenliği, gizliliği ve bütünlüğüne yönelik eylemlerin de çoğunlukla beraberinde gelmesini göz önünde bulundurarak verilerin elde edilmiş olunması şartı aranmaksızın bilişim sistemine hukuka aykırı olarak girilmesi bunun sonucunda bilişim sisteminin güvenliğinin ihlal edilmesini başlı başına bir suç olarak düzenlendiği söylenebilecektir.[886] Bilişim sistemine girme tek başına gerçekleştirilebileceği gibi bilişimle ilgili olsun veya olmasın başka bir suçu

şifre çözücülerin ya da güvenlik yapılarını ortadan kaldıran bilgisayar programlarının üretimi, sağlanması … vs. de ayrıca suç sayılmaktadır.
…5237 sayılı TCK'da, 243. maddesindeki suçla bağlantılı olarak belirtilen örnekler de dikkate alınarak bilişim verilerine yönelik suçların hazırlığına dair suçlara yer verilmelidir." Bkz. Karagülmez, "Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu", s. 253.

886 A.e., s. 805; Apaydın, "Bilişim Sistemine Girme Suçu", s. 253, 254; Parlar ve Hatipoğlu, a.g.e., s. 3741; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 236, 237.
"…Yalnızca bilişim sistemine haksız erişimin dahi başlı başına bir suç olarak düzenlenmesi önemli bir ihtiyaç olarak görülmektedir.
…Dışa açık olmayan bir bilişim sistemine haksız erişim, bilişim suçları içerisinde en çok görülen fiillerden birisidir. Bu fiil, genellikle klasik (geleneksel) suçlarda konut dokunulmazlığının ihlâl edilmesi suçuna benzetilmektedir.
…Bilişim suçlarında haksız erişim, tek başına gerçekleştirilebileceği gibi, bilişimle ilgili olsun ya da olmasın başka bir suçu işlemek için "araç suç" olarak da görülebilir. Hatta haksız erişimin araç suç şeklinde işlenmesi daha yaygındır.
…Haksız erişim, bilişim sistemlerinin kullanıcılarının engellenmesine veya sistemlerde onarılması yüksek maliyetli kayıp veya tahribatlara neden olabilir. Haksız erişimler, aleni olmayan verilere veya sırlara ulaşılmasına, hatta bilişim sistemlerinin bedelsiz kullanılmasına yol açabilir. Haksız erişim, öncelikle fark edilmediği ve sonra da teknik ve yasal önlemlerle engellenmediği takdirde failleri bilişimle ilgili daha başka suçlara teşvik edebilir; yöneltebilir." Bkz. Karagülmez, "Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu", s. 236, 237.
"Yetkisiz erişimlere açık olmayan bir bilişim sistemine hukuka aykırı erişim, bilişim suçları içerisinde en sık görülen eylemlerden biridir. Bu eylem öğretide geleneksel suçlardaki konut dokunulmazlığının ihlali suçuna benzetilmektedir. Bu suç yalnızca sisteme girmek hedeflenerek gerçekleştirilebileceği gibi, bilişimle ilgili olsun ya da olmasın başka bir suç işlemek için "araç suç" olarak da işlenebilir. Bu yönüyle hukuka aykırı erişimin konut dokunulmazlığı suçuna daha fazla benzerlik gösterdiği ifade edilmektedir." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 238.
"Bilişim sistemine hukuka aykırı erişim suçu, bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilecek olan dolandırıcılık veya hırsızlık gibi suçlarla ya da doğrudan bilişim suçları olan TCK'nın 244 ve 245'inci maddelerinde belirtilen suçlara zemin hazırlamakta ve bir araç olarak kullanılmaktadır." Bkz. Apaydın, "Bilişim Sistemine Girme Suçu", s. 254.
"Bilişim sistemine izinsiz girilmesinin suç haline getirilmesi aynı zamanda sistemin içerdiği verilerin dışarıdan gelecek müdahalelere karşı korunmasını da sağlamaktadır. Zira, sisteme izinsiz girmek sistemdeki verilerin varlığı, bütünlüğü ve gizliliği bakımından bir tehlike oluşturmaktadır. Nitekim sisteme girilmesinin verilere zarar vermesi bu suçun neticesi sebebiyle ağırlaşmış hali olarak kabul edilmiştir (m. 243/3). Kanun koyucu esasen sistemin içeriğini daha erken bir safhada korumak amacıyla sisteme girilmesini suç olarak düzenlemiştir." Bkz. Koca ve Üzülmez, a.g.e., s. 808.
"Bilişim sistemine girme suçu öncü bir suç niteliği taşımaktadır. Zira pek çok suç (verileri bozma, yok etmek, değiştirmek, verilerin güvenliğini yani gizliliğini ihlal etmek vs gibi) bilişim sistemine girildikten sonra işlenebilmektedir. Bu bakımdan verilerin ele geçirilip geçirilmediğine bakılmaksızın bu fiilin cezalandırılması bundan sonra işlenebilecek suçları engelleyici bir fonksiyonu yerine getirmektedir." Bkz. . Doğan, a.g.e., s. 40.

işlemek için "araç suç" olarak da görülebilmekte olup bilişim suçları içerisinde en çok görülen fiillerden olması[887] sebebiyle de madde yerinde bir düzenleme olarak kabul edilebilecektir.

243. m., tarafı olduğumuz AKSS' nin "Kanunsuz Erişim" başlıklı 2. m.'sinde yer alan bilişim sistemine yetkisiz erişim suç tipi düzenlemesine (yükümlülüğü) uygun olarak suçun oluşması için sisteme haksız ve kasten girilmesini yeterli görmekle birlikte failin güvenlik önlemlerini ihlal ederek sisteme erişmesi ve bilişim sistemleri aracılığıyla sistemdeki verileri elde etmesi veya zarar vermesi amaçlarıyla hareket etmesi şartını aramamıştır.[888] Sisteme yetkisiz erişim veya girme, mukayeseli hukukta da birçok ülkede suç olarak kabul edilmiş olup örnek olarak Alman Ceza Kanunu'nda 202a, Fransa Ceza Kanunu' nda 323/1, İtalyan Ceza Kanunu' nda 616/2, 617, 618, Danimarka Ceza Kanunu' nda 193 ve 263, Norveç Ceza Kanunu'nda 145/2. m.'lerinde yer verilmiştir.[889]

İncelemekte olduğumuz madde 4 fıkradan oluşmakta olup 1 fıkrada suçun temel şekli düzenlenmiş olup bu suçun unsurları ele alındıktan sonra suçun nitelikli halini oluşturan 2. fıkra ve suçun neticesi sebebiyle ağırlaşmış halini oluşturan 3. fıkra düzenlemesindeki açıklamalara 1. fıkra düzenlemesine atıf yapacak şekilde incelenmiş, 4. fıkrada yer alan veri nakillerini teknik araçlarla izleme ayrı bir suç olarak düzenlendiğinden bilişim sistemine girme veya sistemde kalma suçu üst başlığı içerisinde yer almakla birlikte ayrı bir başlık altında unsurları ile birlikte ayrıca ele alınmıştır.

887 Karagülmez, "Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu", s. 236.

888 Koca ve Üzülmez, a.g.e., s. 806.

889 Parlar ve Hatipoğlu, a.g.e., s. 3742.
"Sisteme yetkisiz girme, değişikliğe giden veya kanunlaştırmaya giden ülkelerin genelinde suç olarak kabul edilmiştir. Bu ülkelere göre, suçun oluşması için sisteme yetkisiz girilmesi yeterlidir. Fransa, Lüksemburg, Hollanda, İngiltere, Amerika Birleşik Devletleri, Norveç gibi.Ancak bazı ülkeler sisteme girmeyi suçun oluşması bakımından yeterli saymayıp, verilerin elde edilmesini de aramışlarsa da (Almanya, Türkiye gibi) bu ülkelere daha sonra yapılan değişikliklerle (Almanya 07.08.2007 – Türkiye 1 Haziran 2005 ve 24.03.2016) verilere erişim (giriş) imkânının sağlanması (Almanya), sisteme girmek suç haline getirilmiştir. Bazı ülkeler ise yetkisiz girme dışında, sistemden çıkarma yetkisine sahip olan kişilerin rızasına aykırı olarak sistemde kalmaya devam edilmesini de suç olarak kabul etmişlerdir. Fransa, Belçika ve İtalya gibi. Bu ülkeler girme ve orada kalmayı seçimlik hareket olarak düzenlemişlerdir…Yukarıda belirtilen ülkelerden bazıları girme dışında verilerde bir zarar meydana gelmesini netice sebebiyle ağırlaşmış suç olarak kabul etmiştir. İtalya, Fransa, Lüksemburg, Norveç gibi. Bazı ülkeler ise fiilin bazı kişiler tarafından işlenmesini nitelikli hal olarak kabul etmişlerdir. (İtalya, Yunanistan)" bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 92, 93.

3.2.1.1. Korunan Hukuksal Değer

Ceza Kanunu' nda suç olarak ihdas edilen her fiil bir hukuksal değerin ihlalini oluşturduğundan incelemekte olduğumuz suç tiplerinin daha iyi anlaşılabilmesi, yorumlanabilmesi ve öneri getirilebilmesi adına öncelikle korudukları hukuksal değerler incelenecektir.[890] Zira, Dülger' in de belirtmiş olduğu gibi modern ceza hukuku öğretisinin temelini oluşturan suçla korunan hukuksal değer kavramının "suç politikası", "suçları gruplandırma", "ceza yaptırımını gerekçelendirme, sınırlandırma ve denetleme", "yorum aracı olma" gibi işlevleri bulunmaktadır.[891] Bilişim sistemine girme suçunun koruduğu hukuksal değer hususunda doktrinde farklı görüşler bulunmaktadır. Bu görüşleri üç gruba ayıracak olursak birinci görüş korunan hukuksal değerin bilişim sisteminin güvenliği olduğunu, ikinci bireyin özel alanı veya malvarlığı alanı olduğunu, üçüncü görüş ise korunan hukuksal değerin karma nitelikte olduğunu ileri sürmektedir.

Birinci görüşü savunan Koca ve Üzülmez' e göre, hayatın her alanında kullanılan bilişim sistemlerine yetkisiz kişilerin girmesinin başlı başına, kişilerde bu sisteme olan güven duygusunu zedeleyerek kişileri bu sistemlerden kaçınmaya itecek nitelikte olduğu bu suçun düzenlenmesi ile bilişim sistemlerinin güvenliğinin korunduğu belirtilmektedir.[892] Dülger'e göre, bu suç ile verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı veya kişilerin veya kurumların ihtiyaç duyduğu güvenlik duygusu gibi birçok farklı hukuksal değer ihlali koruma altına alınıyor olsa da bu suç ile korunan hukuksal değer diğer tüm değerlerin üzerinde ve onları kapsayacak şekilde bilişim sistemlerinin güvenliğidir.[893] Zira, bilgi güvenliği

890 Apaydın, "Bilişim Sistemine Girme Suçu", s. 255.
"Hukuki yarar, suç tipinin ihdas edilmesi ile korunmak istenen değerdir, toplumun ceza hukuku tarafından korunan yaşamsal değerleridir, beşeri bir ihtiyacı gidermeye yarayan veya en azından böyle kabul edilen bireysel, kamusal ve toplumsal her çeşit şeydir şeklinde tanımlanmıştır." Bkz. Doğan, a.g.e., s. 41.
"Kural olarak her norm bir hukukî değeri korur. Ancak birçok norm vardır ki bunlar birden fazla hukukî değeri korurlar. Bunun anlamı her normun bir değerin ihlaline, ancak birçok normun da birden fazla değerin ihlaline karşı konduğudur.
…Birden fazla hukukî değeri ihlal eden suçları her kısım ve bölümde bulmak mümkündür.
…Birden fazla menfaate zarar veren suçları kanun koyucu menfaatlerden hangisi daha önemli ise o menfaate ilişkin bölüme yerleştirmiştir.
…Ancak bu gibi değerlendirmeler çoğu zaman ahlakî, sosyal ve politik nedenlerle değişmekte, çeşitli ülke kanunlarına, hatta bir ülkenin muhtelif zamanlarda yapılan kanunlarına göre bile değişmektedir." Bkz. Soyaslan, a.g.e., s. 70, 71.
891 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 233.
892 Zira, bilişim sisteminin oluşabilmesi için sisteme kasten ve haksız olarak girilmesi yeterli olup sistemdeki verilerin ele geçirilmesi, sistemin veya içerdiği verilerin zarar görmesi şartı aranmadığından bu suçla kişilerin özel hayatlarının gizliliği veya malvarlığı değerlerinin korunduğu söylenememektedir. Ayrıntılı bilgi için bkz. Koca ve Üzülmez, a.g.e., s. 807.
893 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 243, 244.

teknolojilerinin başlı başına bir sektör haline geldiği günümüzde sadece güvenlik sisteminin kırılarak bilişim sistemine girilmesi dahi bu sistemlerin doğruluğuna ve erişilemezliğine olan güveni yok etmektedir.[894] Parlar ve Hatipoğlu da korunan hukuksal değerin bilişim sisteminin güvenliğinin sağlanması olduğunu belirtmekle buna birlikte bilişim sistemini kullananların çıkarlarının zedelenmemesini de eklemektedir.[895] Akbulut' a göre de, kanun koyucu bireylerin müdahalelerinden uzak, rahatsız edilmeden, güven içinde bilişim sistemlerinin kullanılmasını esas alarak bu suç tipi ile bilişim sisteminin güvenliğini ve dokunulmazlığını korumaktadır.[896] Özbek-Kanbur-Doğan-Bacaksız ve Tepe' ye göre de, yasa koyucu tarafından erişimi belli bir yetkilendirmeye dayalı veya güvenceye alınmış olan bir bilişim sistemine yetkisiz erişim engellenmek istendiğinden suçla korunan hukuksal değer bilişim sisteminin güvenliği ve güvenilirliğidir.[897] Mahmutoğlu' na göre de kanun koyucu, artan oranda bilişim sistemleri aracılığı ile yapılan işlem sayısı karşısında bu sistemlerin tercih edilebilmesi için onlara olan güvenin tam olması gerektiği fikrinin esas alarak bilişim sisteminin güvenliğini koruma altına almaktadır.[898]

İkinci görüşü savunan Kurt' a göre TCK 243. m.'sinde düzenlenen suç ile bilişim sistemi ve içinde bulunan verilerin, programların içinde bulunduğu sistem sahibinin özel veya kişisel alanı, başka bir deyişle özel hayatın gizliliği ve sırların

894 A.e.

895 Parlar ve Hatipoğlu, a.g.e., s. 3742.

896 Akbulut, *Bilişim Alanında Suçlar*, s. 118.

897 "Bilişim sisteminin güvenilirliğinden kastedilen şeyi ise şu şekilde özetlemek mümkündür:
Bilişim teknolojisindeki gelişmelere paralel olarak günümüzde bireyler birçok işlemini başta internet olmak üzere farklı bilişim sistemlerini kullanmak suretiyle yerine getirmektedir. Bu açıdan toplumda bu sistemlere karşı bir güven duygusu oluşmaktadır. Ayrıca kişisel kullanıma özgülenmiş bilgisayar gibi bilişim sistemlerinde kişiler, kendilerine özgü ve sadece kendilerinin yönetmek isteyecekleri bir alan oluşturmaktadır. Dolayısıyla bu alanın kişiliklerini rahatlıkla geliştirebilecekleri güvenli bir alan olmasını isteme ve bu güvenliğin korunmasını bekleme hakkına sahiptirler. Şayet kişinin serbestçe üzerinde tasarrufta bulunabileceği verileri kapsayan ve dış etkilere karşı korumaya alınan bir bilişim sistemine, sistem sahibinin rızası hilafına ve hukuka aykırı bir şekilde yetkisiz erişim sağlanırsa, o sisteme karşı güven de ortadan kalkacaktır. Bir ölçüde bilişim alanında işlenen suçların topluma karşı işlenen suçlar kapsamında düzenlenmiş olmasının bir gerekçesi olarak bu bilişim sistemlerine karşı toplumda ortaya çıkan güven duygusunun korunması ihtiyacı gösterilebilir." Bkz. Özbek, v.d., a.g.e., s. 918, 919.

898 Ancak Mahmutoğlu şunları da eklemektedir: "Aslında güvenliğin sağlanmasına yönelik amacın yanı sıra daha sonra oluşabilecek hırsızlık ve dolandırıcılık suçlarının da engellenmesi hedeflenmektedir.
Diğer taraftan bir sisteme hukuka aykırı olarak girilmesi ve orada kalınması ile sistem maliki veya kullanıcısının özel hayatının gizliliği veya dokunulmazlığı, sırlarının masumiyeti, haberleşme hürriyeti gibi farklı türdeki birçok hakkının da ihlali gündeme gelebilir. Söz konusu yasal düzenlemeyle, kişilerin hak ihlallerinin de önüne geçilmek istenmiştir. Bu verilerden hareketle anılan suç tipi ile birden fazla hukuki değerin korunmakta olduğunu söyleyebiliriz." Bkz. Mahmutoğlu, a.g.e., s. 858, 859.

masumiyeti korunmaktadır.[899] Karagülmez ise 243. m.'nin değişiklik öncesi metninde yer alan sisteme girme "ve" kalmaya devam etme hali için maddede suçun unsuru olarak fiilde temadi aranması sonucunda bilişim sistemini kullananların belli bir süre sonra rahatsız edilmemesi, çıkarlarının zedelenmemesi olarak belirtmiştir.[900] Ketizmen' e göre ise, 243. m. malvarlığının korunmasına ilişkin bir düzenleme olup suçun hukuki konusunda malvarlığına ilişkin bir değerin korunması esas alınmış, sırrın korunması veya konut dokunulmazlığının korunması şeklinde ortaya çıkan özel hayatın gizliliğinin korunmasına ilişkin değer ikinci plana itilmiştir.[901]

Üçüncü görüşü savunan Artuk-Gökcen-Yenidünya'ya göre 243. m. ile korunan hukuksal değerin öncelikli olarak bilişim sisteminde yer alan unsurların sahibinin kişisel alanına ait olması sebebiyle bireylerin özel hayatlarının gizliliği, sırlarının masumiyeti, haberleşme özgürlükleri olmasının yanında ikinci bir menfaat olarak bilişim sisteminin güvenliğine yönelen eylemin suç olarak düzenlenmesi bilişim sistemlerine olan itimat duygusu ve bilişim sisteminin güvenliğidir.[902] Yaşar-Gökcan-Artuç' a göre de, bu suç ile sistemde bulunan bilgilerin gizli olması karşısında bir kimsenin bilişim sistemine girildiğinde bilgilerin bilinir hale gelecek ve Anayasa' da koruma altına alınan özel hayatın gizliliği ve serbestçe haberleşme olanağı ihlal edilecektir.[903] Bunun yanında bu suç işlendiğinde bilişim sistemi sahibi veya kullanıcısının zarara uğrama tehlikesi ile karşı karşıya kalması sebebiyle bilişim sisteminin güvenliği ve güvenilirliği, başka suçların işlenmesinin hazırlayıcısı olabileceğinden suç işlenmesinin engellenmesi ve bir diğer değer olarak da malvarlığı değerleri bulunmaktadır.[904] Erdoğan' da 243. m.'nin değişiklik öncesi hali için yani bilişim sistemine girme ve kalma suçu için yapmış olduğu değerlendirme de korunan hukuksal değerin, toplum düzenini korumak, özel hayatın gizliliği, haberleşmenin gizliliği, kullanıcı ve sistem sahibinin menfaatleri, olası başka suçların işlenmesinin önlenmesi, bilişim sisteminin güvenliği olmak üzere karma nitelik taşımakta olduğunu, korunmak istenen asıl değerin ise bunların hepsini içine alan üst değer

899 Kurt, a.g.e., s. 148.
900 Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 182.
901 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 99.
902 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6891.
"Diğer taraftan bir bilişim sistemine girmek ve orada kalmak, sistemi engelleme, bozma, verileri yok etme veya değiştirme ya da bilişim araçları vasıtasıyla işlenecek hırsızlık, dolandırıcılık gibi fiillerin gerçekleştirilmesine zemin hazırlamaktadır. Bilişim sistemine girme, çoğu kez daha sonra işlenecek amaç suçlar için bir araç teşkil etmektedir." Bkz. A.e., s. 6891, 6892.
903 Yaşar, Gökcan ve Artuç, a.g.e., s. 7287.
904 A.e.

olarak bilişim sistemlerine güvenilirliği olduğunu belirtmektedir.[905] Yazıcıoğlu da 243. m.'nin Anayasamızın 20. m.'sinde düzenlenen özel hayatın korunması kavramının bilişim sistemleri kullanılarak ihlalini engelleme isteğinin yanında bilişim sisteminin güvenliği ve mülkiyet hakkını koruma amacı ile düzenlendiğini belirtmektedir.[906] Soyaslan' a göre de bilişim sistemine giren ve orada kalan kişi bir taraftan başkalarına ilişkin veri ya da bilgilere ulaşmakta bu doğrultuda özel hayatın dokunulmazlığını diğer taraftan ise sistemin ulaşılmazlığına olan güveni ihlal etmektedir.[907] Apaydın' a göre de korunan hukuksal değer, bireylerin özel hayatlarının gizliliği, kişisel verilerin güvenliği, iletişim özgürlüğünün korunması, kurumlara ait verilerin güvenliği, kurumların bilişim sistemlerinin güvenli olarak işleyişi, mülkiyet veya zilyetlik haklarının korunması, kamu güvenliği ve kamu düzeninin korunması olmak üzere karma niteliktedir.[908]

Kanaatimizce, 243. m.'sinin birinci fıkrasında düzenlenen suçun temel şeklinin koruduğu hukuksal yararın karma nitelikte olup dar anlamda bireylerin özel hayatlarının gizliliği, kişisel verilerin güvenliği, iletişim özgürlüğünün korunması, kurumlara ait verilerin güvenliği, kurumların bilişim sistemlerinin güvenli olarak

905 Ayrıntılı bilgi için bkz. Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1369-1371.
"Doktrinde bir görüş ise; maddenin TBMM genel kurulundaki tartışmalarına dayanarak burada aslında malvarlığına ilişkin değerlerin korunduğunu, diğer değerlerin ikinci planda kaldığını belirtmektedir. Kanaatimizce maddenin kabulü sırasında TBMM'de yapılan tartışmaların özünde korunmak istenen değerin malvarlığı olduğu değil, 244'üncü maddede düzenlenen ve toplumsal güvenlik, güvenilirlik ve yukarıda saydığımız diğer değerlerin ihlalleri bakımından daha ağır olan eylemlerin cezasının 243'üncü maddeye göre daha hafif kalmasının önüne geçilmek istenmesidir. Dolayısıyla, bize göre, burada korunmak istenen değerlerden birinin de malvarlığı değerleri olduğu doğrudur (biz bunu sistem sahibinin ve kullanıcının menfaatleri başlığı altında değerlendirmeyi uygun görüyoruz) ancak bu tek veya birinci değer değildir. Korunmak istenen asıl değer yukarıda saydığımız tüm değerleri içinde barındıran sistemin güvenilirliğidir." Bkz. A.e., s. 1373. Aynı yönde bkz. . Doğan, a.g.e., s. 43, 44.
906 "Bu sebepledir ki "bilişim sistemine hukuka aykırı olarak girme" fiilini yeni bir suç tipi yaratarak koruma alanı oluşturmak yerine bazı ceza kanunları klasik suç tiplerinden konut dokunulmazlığını ihlâl suçu içinde yaptırım altına almaya çalışmaktadırlar.
Görüldüğü üzere bilişim sistemine hukuka aykırı girme fiillerinin engellenmesi ile artık sadece özel hayatın gizliliğine müdahale edilmesi değil hem ekonomik hem de sosyal bir değer taşıyan sisteminin güvenliğinin de korunması temel ilke teşkil etmektedir." Bkz. Yılmaz Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", Ord. Prof. Dr. Sulhi Dönmezer Armağanı, Cilt II, *Atatürk Kültür, Dil ve Tarih Yüksek Kurumu Atatürk Araştırma Merkezi Türk Ceza Hukuku Derneği*, Ankara, Şubat 2008, ss. 1239-1261, s. 1254.
907 Soyaslan, a.g.e., s. 635.
908 "Bilişim sistemleri eğitim, sağlık, ticaret, ulaşım, iletişim ve hukuk alanlarında bireylerin ve toplumun yaşamında önemli bir noktaya ulaşmıştır. Bu sistemlerin güvenle işleyişi, aynı anda hızlı ve kolayca birçok kişi tarafından ulaşılması, eğitim, sağlık, ticaret, ulaşım, iletişim ve hukuki hizmetlerin sağlanması, kamu güvenliği ve düzenini koruma açısından korunmaya muhtaç bir alandır." Bkz. Apaydın, "Bilişim Sistemine Girme Suçu", s. 258.
Gül' e göre de: "Korunan hukuki yarar karma nitelikli olup, öncelikli olarak 'bilişim sisteminin güvenliği' korunmuş; ayrıca 'özel hayatın gizliliği', 'haberleşme özgürlüğü', 'kişilerin ya da kurumların duyduğu güvenlik duygusu' gibi hakların ihlalleri de önlenmek istenmiştir." Bkz. Gül, a.g.e., s. 59.

işleyişi, mülkiyet veya zilyetlik haklarının korunması geniş anlamda ise bilişim sisteminin güvenliği ve güvenilirliği korunarak bu bağlamda kamu güvenliği ve kamu düzeninin korunması hedeflenmektedir. Zira Apaydın' ın da belirtmiş olduğu[909] gibi günümüzde eğitim, sağlık, ticaret, ulaşım, iletişim ve hukuki hizmetlerin birçoğunun bilişim sistemleri üzerinden sağlanması kamu hizmeti niteliği de taşıyan bu hizmetlerin oluşturduğu alanın dolayısıyla da kamu güvenliği ve düzeninin korunması ihtiyacını doğurmaktadır. Bir suç birden fazla hukuksal değeri ihlal edebilecek olsa da maddenin düzenlendiği bölüm ve kısım, maddenin koruduğu hukuksal yarardan öncelikli olana göre belirlenmektedir. Yukarıda yapmış olduğumuz açıklamalarda da belirtildiği üzere bilişim suçlarının çoğunun sisteme girilmek suretiyle başlaması, sistem ve içerdiği verilerin güvenliği, gizliliği ve bütünlüğüne yönelik eylemlerin de çoğunlukla beraberinde gelmesi göz önünde bulundurarak verilerin elde edilmiş olunması şartı aranmaksızın bilişim sistemine hukuka aykırı olarak girilmesi ile öncelikli olarak bilişim sisteminin güvenliğinin ihlaline engel olma esası bulunmaktadır. Bunun yanında, bu suç tipinin TCK' nın ikinci kitabının "Topluma Karşı Suçlar" başlıklı kısmında ve "Bilişim Alanında Suçlar" başlıklı 10. Bölümünde düzenlenmiş olması da bireysel çıkarlardan ziyade toplum çıkarının ön planda tutulmak istendiğinin göstergesini oluşturmaktadır. Bu durum, "bilişim alanında suçlar" bölümünde düzenlenen suç tiplerinde bireysel hukuki yararların korunmadığı anlamına gelmemekte olup söz konusu suç tipinin bilişim sistemlerinde gerçekleştirilen eylemler ve oluşan suçlar açısından temel olması açısından koruduğu öncelikli hukuksal değerde toplumun bilişim sistemlerine karşı genel güvenlik duygusunun dikkate alındığı belirtilmelidir. O halde, bilişim sisteminin güvenliğinin korunduğu suçların, toplumu ilgilendiren suçlar içerisinde kabul edilmesi de en doğal sonuçtur. Ayrıca 243. m.'nin 2. fıkrasında suçun konusunun "bedeli karşılığında yararlanılabilen sistem" olması halinde cezada indirim gerektiren nitelikli hal olarak belirlenmesi, 3. fıkrada ise bilişim sistemine hukuka aykırı girme veya kalma fiili sonucunda verilerin değişmesi ya da yok olmasının neticesi sebebiyle ağırlaşmış hal olarak düzenlenmesi, suçun temel şekli ile korunan hukuksal değerin değişimi halinde uygulanacak ceza miktarının da değiştiğini göstermekte olup 2. fıkrada ilgilisinin malvarlığının korunmasına yönelik hukuksal değerin daha ön planda olduğu bu anlamda da toplum yararına göre daha az korunacağı esasından hareketle daha az ceza

909 Bkz. Dipnot. 910.

tayin edilmesi, 3. fıkrada ise suçun temel şeklinde korunan hukuksal yarar bilişim sisteminin güvenliği yanında verilerin gizliliği ve güvenliğinin de korunması başka bir deyişle suçun temel şekli ile korunan hukuksal değere eklenmesi sebebiyle daha ağır ceza gerektiren hal olarak düzenlenmesi görüşümüzü destekler niteliktedir.[910]

3.2.1.2. Maddi Unsur

3.2.1.2.1. Fail ve Mağdur

Madde düzenlemesine bakıldığında, kanun koyucu hem fail hem de mağdur açısından bir özellik aranmamış olup bu suç açısından herkes suçun faili veya mağduru olabilecektir. Mağdur açısından, üçüncü kişilerin erişimine kapalı olan suçun konusunu oluşturan bilişim sistemi üzerinde hak sahibi olunması kriteri esas alınmıştır.[911] Bu suç ile bilişim sistemine hukuka aykırı olarak girilmesinden veya orada kalınmasından dolayı hakları tehlikeye girebilecek olan birden fazla mağdur oluşabilecektir.[912] Fail bakıldığında ise, tüzel kişiler suçun faili olamamakla birlikte bu suçun tüzel kişi yararına işlenmesi suretiyle haksız menfaat sağlanması halinde TCK' nın 246. m.'si uyarınca bunlara özgü güvenlik tedbirlerine hükmolunacaktır.[913]

3.2.1.2.2. Suçun Konusu

243. m.'nin birinci fıkrasında yer alan suçun konusunu "bilişim sistemi", ikinci fıkrasında yer alan suçun konusunu "bedeli karşılığında yararlanılan bilişim sistemi", üçüncü fıkrada düzenlenen suçun konusunu "bilişim sisteminin içerdiği veriler", dördüncü fıkrada yer alan suçun konusunu ise "nakledilen veriler" oluşturmaktadır.[914]

---

910 "…suç tiplerinin oluşturulmasında ve düzenlenmesinde esas alınan unsur suçla korunan hukuksal değerdir. Bu öğretinin önemli etkilerinden biri de suç politikası kapsamında suçlara karşılık verilecek yaptırımların belirlenmesi ve dolayısıyla hangi durumların ağırlatıcı ve/veya hafifletici hal olarak tanımlanacağının belirlenmesidir. Buna göre tek bir hukuksal değer ihlal edildiğinde bir birim ceza veriliyor iken, iki farklı hukuksal değerin ihlali halinde iki birim ceza verilmesi gerekir…" bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 269.

911 Yaşar, Gökcan ve Artuç, a.g.e., s. 7288; Özbek, v.d., a.g.e., s. 920.

912 "Örneğin; bir kimsenin kişisel dosyasını arkadaşının bilgisayarında muhafaza ettiği düşünülürse, bu bilgisayara girilerek söz konusu dosyaya ulaşılması halinde de hem bilgisayarın sahibinin hem de veri sahibinin mağdur olduğu şüphesizdir." Bkz. Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1395.

"Başkasının bilgisayarında üçüncü kişilerin kişisel dosyasına ulaşılması, bankanın sistemine girilerek müşteri hesaplarının incelenmesi, bir şirketin MSN hesabına girilerek üçüncü kişilerin bilgilerinin öğrenilmesi durumunda ilgililerin de suçun mağduru olabileceği kabul edilmekle birlikte, bu durumda TCK 135, 136. maddelerinde yazılı kişisel verilerin hukuka aykırı olarak ele geçirilmesi (örneğin, üçüncü bir kişinin kişisel bilgilerinin elde edilmesi gibi) ve verilerin hukuka aykırı olarak başkasına verilip yayılması suçları da göz önünde tutulmalıdır." Bkz. Gül, a.g.e., s. 61.

913 Koca ve Üzülmez, a.g.e., s. 807; Yaşar, Gökcan ve Artuç, a.g.e., s. 7288.

914 Yaşar, Gökcan ve Artuç, a.g.e., s. 7288.

"Bilişim sistemi" ve "veri" kavramı birinci bölümde ayrıntılı olarak incelendiğinden bu başlık içerisinde ismen değinilmekle yetinilecek olup diğer fıkralarda yer alan suçların maddi konularına ilişkin açıklamalara ise ilgili başlıklar altında yer verilecektir.

Bu başlık altında değinmek istediğimiz husus şu ki TCK' nın 243. m.'sinde düzenlenmiş olan suçun maddi konusunu oluşturan bilişim sistemlerinin kamu veya özel hukuk tüzel kişisine ve hatta gerçek kişiye ait olup olmaması bakımından bir ayrım yapılmamasının suçla mücadele açısından bir eksiklik oluşturduğudur. Nitekim, ABD' de bilişim suçlarının düzenlenmiş olduğu temel kanun olan Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Yasası' nda (Computer Fraud and Abuse Act - CFAA) konu ayrıntılı olarak düzenlenerek suçun konusunu oluşturan bilişim sisteminin niteliğine göre farklı yaptırımlar öngörülmüştür.[915] Bu bağlamda, kamu kurumlarının bilişim sistemlerine gerçekleştirilen hukuka aykırı girme veya kalma fiilinin cezayı artıran nitelikli hal olarak düzenlenmesi uygun olacaktır.[916] Bir başka husus ise doktrinde, 243. m.'nin 3. fıkrasında yer alan bilişim sistemine hukuka aykırı girme veya kalma eylemi sonucunda yok olan veya değişen verinin önemi ve niteliğinin gözetilmesi gerektiğine ilişkin görüşler[917] bulunmakta ise de kanaatimizce verinin önem derecesini belirleme kıstası muğlak olduğundan ve hakimin takdirine göre değişebileceğinden ceza hukuku ilkelerinden olan belirlilik kavramını zedeleyebilecek niteliktedir bunun yanında ceza mevzuatımız açısından bakıldığında da verinin ilişkin olarak sistem içindeki her türlü soyut unsur olarak kabulü, önem ayrımı kıstası eğiliminde olunmadığı görüldüğünden söz konusu madde kapsamında

915 Karagülmez, "Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu", s. 250.
"CFFA'da göze çarpan önemli bir özellik siber suçların hedef sistemin özelliği bakımından ayrıştırılmasıdır. Bu maksatla kanunda koruma altındaki bilgisayar (protected computer) kavramına yer verilmiştir. Yapılan tanıma göre koruma altındaki bilgisayar "(1) finansal bir kurum ya da devlet kurumlarına münhasıran kullanılan veya bunlarca dolaylı olarak kullanılıp suç fiilinin bunları etkilediği veya(2) ABD dışında da olsa eyaletler arası ya da uluslararası ticaret veya iletişim maksadıyla kullanılan bilgisayardır." Bazı mahkeme kararlarında ağ üzerinde çalışan her bilgisayar koruma altındaki bilgisayar kavramı kapsamına sokulsa da, kanunun özünde böyle bir ayrıma yer verilmesi önemlidir. Kanunda bulunan diğer bir özellik siber suçları ve öngörülen cezaları failin motivasyonuna göre de ayrıştırıyor oluşudur. Aynı şekilde diğer bir olumlu yön kanunda yorum farklılığına sebebiyet vermemek maksadıyla bilgisayar, finansal kurum, zarar, kayıp gibi pek çok temel kavramın tanımlarına yer verilmesidir." Bkz. Hekim ve Başıbüyük, a.g.e., s. 151.
916 Aynı yönde görüşler için bkz. Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1400; Apaydın, "Bilişim Sistemine Girme Suçu", s. 272; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 272.
917 Karagülmez, "Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu", s. 250.

bilişim sistemleri açısından yapılacak ayrımın gerekli ve yeterli bir düzenleme olacağı düşüncesindeyiz.

3.2.1.2.3. Fiil

TCK 243. m.'nin 1. fıkrasında yer alan suç tipinde 6698 sayılı Kanun ile gerçekleştirilen değişiklik neticesinde bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girmek veya orada kalmak seçimlik hareketlerinden birinin gerçekleştirilmesi ile suç oluşmaktadır.[918] Suçun oluşması için ayrıca bir neticenin gerçekleşmesi şartı aranmadığından sırf hareket suçu olarak kabul edilecek olan suç[919], kalma eylemi ihmali hareket özelliği de gösterebildiğinden hem icrai hem de ihmali hareketle işlenebilmektedir.[920] Bunun yanında, failin bilişim sistemine girmesi veya kalmaya devam etmesi ile bilişim sisteminin veya içerdiği verilerin herhangi bir zarara veya zarar tehlikesi ile karşılaşmasına gerek olmadığından bu suç soyut tehlike suçu olarak[921], suçu meydana getiren hareket ise tanımlanmadığından başka bir deyişle girme ve sistemde kalmaya yarayacak her fiil yöntemi ne olursa olsun madde kapsamı içine alınmış olduğundan bu suç serbest hareketli bir suç olarak kabul edilecektir.[922]

Doktrinde, girme ve orada kalma eyleminin bilişim sisteminin sanal alanının içerisine girilmesi olduğu bu eylemlerin bilgisayarın açılması suretiyle verilerin görünmesi şeklinde olabileceği (fiziksel) gibi bir ağ aracılığı ile bilişim sisteminde

---

918 Koca ve Üzülmez, a.g.e., s. 811.

919 Apaydın, "Bilişim Sistemine Girme Suçu", s. 265.
Yargıtay 8. Ceza Dairesi' nin kararında: "…Şikayetçinin rızası olmadan e-mail ve Facebook hesabına girip şifrelerini değiştirmek suretiyle bilişim sistemine girmesini engellediğinden bahisle açılan davada; katılanın hesabına sanığın giriş yaptığının tespit edildiği, dosya içerisinde şifrelerinin değiştirilmesine dair bir tespitin bulunmadığı ve katılanın hesabının kullanılarak kontör istenen arkadaşları olduğu anlaşılmakla, kalmaya devam ettiğine ilişkin deliller de mevcut olduğundan, sanığın eyleminin TCK'nın 243/1. maddesi kapsamındaki suçu oluşturacağı gözetilmeden suç vasfında yanılgı sonucu yazılı şekilde hüküm kurulması, … BOZULMASINA" Yargıtay 8. Ceza Dairesi, 6.12.2017 t., E: 2017/7826, K: 2017/13823, https://www.hukukmedeniyeti.org/ictihat/877255/, ET. 15 Temmuz 2020.
Benzer yönde bkz. Yargıtay 8. Ceza Dairesi, 29.11.2017 t., E: 2017/10095, K: 2017/13454; Yargıtay 8. Ceza Dairesi' nin 3.11.2014 t., E. 2014/21702, K. 2014/24201.

920 Akbulut, *Bilişim Alanında Suçlar*, s. 128.

921 Yaşar, Gökcan ve Artuç, a.g.e., s. 7294.

""…… Sanığın katılanın yetkilisi olduğu Z… Tekstil Şirketi'nin T… Bankası D… Şubesi'nde bulunan hesabına internet üzerinden izinsiz giriş yaptığı ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında, sanığın eyleminin 5237 s. TCK'nın 243/1. maddesinde düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde (5237 s. TCK'nın 244/4, 35/2 maddeleri gereğince) hüküm tesisi…" 11. CD. 26/03/2009 gün, 2008/18190 E-2009/3058 K" https://legalbank.net/arama, ET. 15 Temmuz 2020; bkz. Gül, a.g.e., s. 64; Ömer Demir, Mehmet Arıç ve Halil Polat, *Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar : Soruşturma ve Kovuşturma Yöntemleri*, Adalet Yayınevi, Ankara, 2015, s. 9.

922 Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1378.

oturum açılması yolu ile de gerçekleştirilebileceği belirtilmektedir.[923] "Girmek" ifadesinden ise "bilişim sistemlerinin oluşturduğu dijital alana girmek" başka bir

923 "Giriş kablolu, kablosuz bağlantı ile olabileceği gibi kızılötesi ışınlar ile de olabilir; hatta bluetooth gibi sistemler marifetiyle veya manuel olarak yani doğrudan bir bilişim sistemi ile fiziki temasa geçerek sistemi kullanmak suretiyle sisteme girmek şeklinde cereyan edebilir." Bkz. A.e., s. 1379.
"Bilişim sistemine girme hareketinin gerçekleştirilmesi bakımından herhangi bir sınırlama söz konusu değildir. Bu konuda çeşitli ihtimaller düşünülebilir. İlk olarak, bilişim sistemine girme ağ üzerinden ulaşılarak girilebileceği gibi, manuel olarak da ulaşılabilir. Bu ikinci durumda fail, sisteme fiziki olarak müdahale etmektedir…Diğer bir ihtimalde sistemin dâhil bulunduğu ağa müdahale ederek, sistemin veri nakli sırasında ağa gönderdiği verilere ulaşılması söz konusudur." Bkz. Artuk, Gökcen, Yenidünya, Türk Ceza Kanunu Şerhi: Madde 234-345, s. 6895.
Yargıtay 8. Ceza Dairesi'nin 3.2.2015 tarihli, E:2014/19342, K:2015/2322 sayılı kararında:
" "Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Suçun, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır.
E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikayeti üzerine öncelikle erişimi engellenen adresin ve sanığa ait olduğu iddia olunan e-mail adresinin sanığa ve şikayetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adreslerin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (İnternet Protokolu) numarası sorulmalıdır. Microsft Corporation'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde şikayetçinin e-mail adresine giriş yapıp yapmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli, aynı şekilde sanığa ait olduğu iddia olunan e-mail adresini kullanan IP numaraları saptanıp adres ve telefon bilgileri de istenmelidir.
Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şikayetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.
Şikayetçi ve sanığın bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp ele geçirilen adresten bir başka adrese yazı veya görüntü gönderilmiş ise, bu olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak ulaşılan adres sahipleri varsa tanık olarak dinlenmelidir.
Somut olayda; sanığın, katılanın kullandığı "...@hotmail.com" e-posta adresi ile irtibatlı olan facebook adresine bilgisi ve rızası olmaksızın değiştirerek erişilmez kıldığından bahisle açılan davada, yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan mahkumiyet hükmü kurulmuştur. Sanığın suçlamayı kabul etmediği gibi hattına başkalarının girmiş olabileceği savunmasına ilişkin olmak üzere internet hattını sanık dışında başkalarının da kullanıp kullanmadığı ve kendisine ait olduğu belirtilen e-mail adresinin sanığa aidiyeti hususunda dosyada bir bilgiye rastlanmamıştır. Katılanın 27.05.2011 tarihinden itibaren e-mail adresine giremediğini belirttiğinin anlaşılması karşısında, anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, katılan tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit edilmemiştir. Sanık tarafından 22.05.2011 tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulmadan hüküm kurulmuştur.

deyişle soyut, sanal alana girmek kastedilmektedir.[924] Bunun yanında "girmek" fiili yerine "erişmek" ifadesinin kullanılmasının daha uygun olacağına ilişkin görüşler[925] bulunmakta olup kanaatimizce de madde ile korunmak istenen değer ve maddenin düzenleniş amacı dikkate alındığında ve doktrinde "girmek" fiili açıklanırken bir bilişim sisteminin sanal ortamına veya alanına, sayısal unsurlarına, içeriğine yetkisiz olarak erişmek, ulaşmak ifade edildiğinden madde düzenlemesinde terminoloji açısından izinsiz veya yetkisiz erişim ifadesinin kullanılması daha uygun olacaktır.[926]

Bu itibarla; yukarıda açıklanan yöntem izlenerek eksiklikler yerine getirilip sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, katılanın beyanına itibar edilerek ve eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması," şeklinde yer vermiş olduğu gerekçe de bu yöndedir. https://legalbank.net/arama, ET. 15 Temmuz 2020.

Benzer yönde bkz. Yargıtay 8. CD., 11.3.2015 t., E: 2014/29566, K: 2015/13421; Yargıtay 8. CD., 6.12.2017 t., E.2017/7105, K. 13811; Yargıtay 8. CD., 17.9.2019 t., E: 2018/11841, K: 2019710745; Yargıtay 12. CD., 20.4.2016 t., E: 2015/7248, K: 2016/6819;

Yargıtay 8. CD.' nin 7.9.2019 tarihli, E: 2018/10307, K: 2019/10751 sayılı kararında da:

"…Somut olayda; şikayetçi ... vekilinin 27.09.2016 tarihinde İstanbul Cumhuriyet Başsavcılığına başvurarak müvekkilinin whatsapp programına casus program yerleştirilerek konuşmalarının dinlendiğini, şikayet dilekçesine ekli belgede de gösterildiği gibi kendi yaptırdıkları uzman incelemesine ve İstanbul İl Emniyet Siber Suçlarla Mücadele Şube Müdürlüğünün 10.04.2018 tarihli soruşturma evrakına göre şikayetçinin whatsapp uygulamasına program yerleştirildiği ve programı yerleştirenlerin İstanbul'un F. ilçesinde bulunduğu ve whatsapp programına casus yazılım aracılığıyla erişim sağlayan IP adresinin şikayetçinin daha önce genel müdürlüğünü yaptığı ve husumetli şekilde ayrıldığı ... Vakfı isimli kuruluşa ait olduğunu bildirmesi karşısında adı geçen vakfın suçun işlendiği süreçteki yetkilileri tespit edilerek ifadelerine başvurulması ve tespit edilen şahıslarca söz konusu eylemin yapılıp yapılmadığının tespitine yönelik teknik araştırma yapılması ayrıca şikayetçinin de ayrıntılı beyanına başvurularak sonucuna göre şüpheli ye da şüphelilerin hukuki durumlarının değerlendirilmesi gerekirken eksik soruşturma ile verilen kovuşturmaya yer olmadığına ilişkin karara yönelik itirazın kabulü yerine yazılı şekilde karar verilmesi," şeklinde karar verilmiştir. Bkz. https://legalbank.net/arama, ET. 15 Temmuz 2020.

924 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 259; Malkoç, a.g.e., s. 2069; Gül, a.g.e., s. 63.

Yargıtay 11. Ceza Dairesi bir kararında: "…müdahil şirkete ait decoder dışında özel bir alet yardımıyla çözüldüğü saptanamadığına göre, abonelik sözleşmesiyle evinde kullanmak üzere alınan decoderin, sözleşme hükümlerine aykırı olarak başka yerde kullanılmasından ibaret eylemin hukuki nitelikte bulunduğu gözetilmeden yazılı şekilde hüküm kurulması, … BOZULMASINA" hükmetmiştir. Bkz. Yargıtay 11. Ceza Dairesi, 13.4.2009 t., E: 2006/7779, K: 2009/4153, https://legalbank.net/arama, 15 Temmuz 2020.

925 "Öğretide "girme" yerine "erişim" kavramının kullanılmasının daha uygun olacağı, zira eylemin sanal ortama yönelik olduğu ifade edilmektedir. Nitekim 5651 sayılı Yasaya dayanılarak çıkarılan "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik"in 3/1-e maddesinde ve "İnternet Toplu Kullanım Sağlayıcılar Hakkındaki Yönetmelik"in 3/1-c maddesinde "erişim" kavramı kullanılmış ve "erişim" her iki düzenlemede de "Herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılmasını ifade eder" şeklinde tanımlanmıştır. Böylelikle öğretideki görüş de desteklenmiş olmaktadır. Ben de girme yerine erişim sözcüğünün daha uygun olduğunu düşünmekteyim." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 259.

926 Aynı yönde bkz. Mahmutoğlu, a.g.e., s. 860, 861; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 260, 261.

"Çalışan bilişim sistemi aracının sanal alanının içine girmedir…Diğer bir deyişle, girmek kavramı bilişim sisteminin yazılımla ilgili bölümünün tamamına veya bir kısmına ulaşmak, dâhil olmak, erişmek anlamına gelmektedir.

Nitekim, 243. m.'nin başlığında tercih edilen "bilişim sistemine girme" suçu mukayeseli hukukta "yetkisiz erişim", "zorla erişim", "hileyle erişim" gibi farklı kavramlarla kullanılmakta[927] olup Avrupa Siber Suç Sözleşmesi'nin 2. m.'sinde öngörülen hukuka aykırı erişim suç tipi düzenlemesi de dikkate alındığında gerçekleştirilecek olan değişiklikle mukayeseli hukukla uyumlu bir düzenleme oluşacağı açıktır. Kalmaya devam etmek için bir süre süre sınırlaması bulunmayıp kalmaya devam etmenin suç oluşturması için mutlaka sisteme hukuka aykırı giriş yapılmış olması şartı aranmamaktadır.[928]

Suçun oluşabilmesi için bilişim sistemine girişi engelleyici tedbirlerin alınması şartı aranmamakta olup hukuki sınırların varlığı yeterlidir.[929] Hukuki sınırların varlığından kasıt ise sistem sahibi tarafından sisteme girilmesine izin verilmemesi[930] olup herkes tarafından istenildiğinde erişilebilen bir bilişim sistemi için söz konusu suç oluşmayacaktır.[931] Bunun yanında bir bilişim sisteminin tamamı veya bir kısmına

…"Erişim", bilgisayar sisteminin tamamına ya da bir parçasına (donanım,bileşenler,yüklenen sistemin saklanan verileri,dizinler,trafik ve içerikle ilişkili veriler) girilmesi anlamındadır…" Bkz. Apaydın, "Bilişim Sistemine Girme Suçu", s. 262, 264.

927 Karagülmez, "Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu", s. 236.

928 Bu anlamda hukuka uygun giriş yapıldıktan sonra hukuka aykırı olarak sistemde kalmaya devam edilmişse suç yine oluşacaktır. Bkz. Akbulut, Bilişim Alanında Suçlar, s. 136.

929 Akbulut, *Bilişim Alanında Suçlar*, s. 132-134; Koca ve Üzülmez, a.g.e., s. 813.

930 "Sanığın soruşturma aşamasında müdafii huzurunda alınan beyanında katılan şirketten ayrıldıktan sonra katılan şirkete ait bilgisayar programına girdiğini kabul etmesi ve değişik zamanlarda bu programa girdiğinin dosya içerisindeki belgelerden anla- şılmış olması karşısında, sanığın oluşan eylemi nedeniyle bilişim sistemine izinsiz girme suçundan TCK.nun 243, 43. maddeleri gereğince cezalandırılması yerine dosya içeriğiyle uyuşmayan gerekçelerle beraat kararı verilmesi, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 4.6.2014 t., E: 2014/3984, K: 2014/13848, https://legalbank.net/arama, 15 Temmuz 2020.

Yine sanığın ayrılmış olduğu katılan şirkete ait mail adresine izinsiz girdiği de iddia olunan eylem hakkında Yargıtay 15. CD'nin 20.3.2019 tarihli, E: 2017/5029, K: 2019/2510 tarihli kararında: "Sanığın katılanın mail adresine izinsiz girdiği iddia olunan eyleminin, sübutu halinde TCK'nın 243/1. maddesinde düzenlenen bir bilişim sisteminin tamamına veya bir kısmına izinsiz girmek suçunu oluşturabileceği de göz önünde bulundurularak, sanık tarafından novatercüme bürosunun mail adresine 06/04/2012 tarihinden sonra giriş yapılıp yapılmadığı, sanığın teklifleri iş yerinde çalıştığı sırada öğrenip öğrenmediği, sanığın katılanın teklifini nerden öğrendiği, sanığın hangi IP numarası ile katılanın email adresine erişim sağlayıp sağlamadığının ilgili internet sağlayıcısından sorulup, gerekirse taraflara ait bilgisayarlar da incelenerek tüm deliller toplanıp gerektiğinde uzman bilirkişiden de görüş alınması, ayrıca sanığın katılanın işyerinde çalıştığı 30/12/2010 - 06/04/2012 tarihleri arasında hangi statü ile çalıştığı, işyerinde görev ve yetki tanımı yapılıp yapılmadığının, sanığa iş yerindeki bilgisayarı kullanma ve müşteri bilgilerine ulaşma ve müşterilere teklif veme yetkisi verilip verilmediğinin tereddüte yer vermeyecek şekilde tespit edilmesi amacıyla, suç tarihinde katılanlara ait şirkette çalışan kişilerin tespit edilerek sanığın yetkisinin kapsamı hususunda ve iş yerinde ki bilgisayarlara ait mail şifrelerinin sanıkta bulunup bulunmayacağı hususunda tanık olarak dinlenilmesi ve sonucuna göre sanığın hukuki durumunun tayin ve takdiri gerekirken yazılı şekilde hüküm kurulması," bkz. Yargıtay 15. Ceza Dairesi, 20.3.2019 t., E: 2017/5029, K: 2019/2510, https://legalbank.net/arama, 15 Temmuz 2020.

931 Koca ve Üzülmez, a.g.e., s. 813.

"Her şeyden önce söz konusu bilişim sistemine erişimin bir takım tedbir veya uygulamalarla sınırlandırılmış olması gerekmektedir. Burada sınırlandırmadan kastedilen şey, bilişim sisteminin

girme arasında suçun oluşumu açısından bir fark gözetilmemiş olup sanal bellek, disket, CD gibi veri taşıyıcısına girmek de bilişim sistemine girme suçunu oluşturabilecektir.[932]

3.2.1.3. Manevi Unsur

TCK 243. m.'sinde yer alan suç için genel kastın varlığı gerekli ve yeterli olup suçun oluşması bakımından özel kastın varlığı aranmamıştır.[933] Failin, giriş izni veya yetkisi olmadığını bildiği bir sisteme bilerek ve isteyerek girmesi veya orada kalması halinde bu suç oluşacaktır.[934] Bu doğrultuda suçun taksirle işlenmesi mümkün değildir. Diğer taraftan suç tipinde hukuka özel aykırılık arandığından bu suç olası kast ile işlenemeyecek olup ancak doğrudan kast ile gerçekleştirilebilecektir.[935]

243. m.'nin 3. fıkrasında düzenlenmiş olan suçun neticesi sebebiyle ağırlaşmış halinin gerçekleşebilmesi için ise failin kasten hukuka aykırı olarak girmiş olduğu bir bilişim sisteminin bütünü veya bir kısmında yer alan verilerin, değişmesi veya yok olması sonucu bakımından taksirle hareket etmiş olması gerekmektedir.[936] Başka bir anlatımla, failin bilişim sistemine girmeyi ve orada kalmayı istemesi ancak verilerin yok olmasını veya değiştirilmesini öngörmesine karşın istememiş olması gerekir.[937]

---

işleyişinin ancak, işlem yapma yetkisine sahip kişilerce gerçekleştirilebilmesidir. Böyle bir yetkilendirmeye en bariz örnek, şifrelendirilmiş bilişim sistemleri olarak gösterilebilir…Dolayısıyla herkes tarafından arzu edildiği her an erişilebilen bilişim sistemleri TCK m. 243/1'in konusunu teşkil etmemektedir." Bkz. Özbek, v.d., a.g.e., s. 922.

932 Akbulut, *Bilişim Alanında Suçlar*, s. 132.

933 Parlar ve Hatipoğlu, a.g.e., s. 3744.

934 Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", s. 1258.

935 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6910; Akbulut, *Bilişim Alanında Suçlar*, s. 139.

Yaşar, Gökcan ve Artuç' a göre ise, bu suç doğrudan kastla işlenebileceği gibi olası kastla da işlenebilir. Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7295.

Özbek, Kanbur, Doğan, Bacaksız ve Tepe' ye göre de bu suç genel kastla işlenebilen bir suç olmakla birlikte olası kastla da işlenebilmektedir. Bkz. Özbek, v.d., a.g.e., s. 927.

936 "Ancak fail bu girme ve kalma fiilinden başka kasten sistemdeki verileri yok edecek veya değiştirecek olursa, artık Kanunun 243/3 üncü maddesindeki netice sebebiyle ağırlaşmış hâl değil, Kanunun 244/2 maddesindeki "sistemdeki verileri yok etme" yani "bilişim sistemindeki verilere zarar verme" suçu gerçekleşir." Bkz. A.e.

937 Yazara göre bu durumda TCK' nın 243/3. maddesindeki suç değil, 244/2. maddedeki suç oluşacaktır. Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7295. Aynı yönde bkz. Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", s. 1259; Mahmutoğlu, a.g.e., s. 863; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6911.

Ancak Özbek, Kanbur, Doğan, Bacaksız ve Tepe' ye göre, "…madde metninde suçun taksirle işlenebileceği açıkça düzenlenmediği için bu imkânsızdır. Dolayısıyla düzenlemenin mevcut hali bakımından TCK m. 243/3'ün de kasten işlenebilen bir suç olduğu, bunun yanında suçun olası kastla da işlenebileceği fakat taksirle işlenemeyeceğinin vurgulanması gerekmektedir." Bkz. Özbek, v.d., a.g.e., s. 928.

3.2.1.4. Hukuka Aykırılık

Suçun kanuni tanımında, bir bilişim sistemine hukuka aykırı olarak girilmesi arandığından failin işlediği fiilin haksızlık teşkil ettiğini biliyor olması aranmaktadır.[938] Başka bir anlatımla, hukuka özel aykırılık oluşturan söz konusu madde ile failin kastı suçun oluşumu için yeterli olmayacak failin hukuka aykırı davrandığı bilinç ve şuuruna da sahip olması gerekecektir.[939] Mağdurun hukuken geçerli rızası, Ceza Muhakemesi Kanunu' nun 134 ve 135. m.'leri uyarınca hakim kararı ile söz konusu fiillerin gerçekleştirilmesi gibi kanun hükmü veya amirin emrinin yerine getirilmesi hallerinde ise suç oluşmayacak ve eylem hukuka uygun sayılacaktır.[940]

3.2.1.5. TCK madde 243 ile Diğer Suçlar Arasındaki İlişki

TCK' nın 243. m.'si ile birlikte bir başka suçun işlenmesi halinde sorunun çözümü için doktrinde farklı görüşler bulunmaktadır. Bir diğer görüşe göre ise, bilişim sistemlerine hukuka aykırı olarak girilerek işlenen suç tiplerinde failin elde etmek istediği amaca yönelik eylemlerini gerçekleştirebilmek için öncelikle üzerinde eylemlerini gerçekleştireceği bilişim sistemine hukuka aykırı olarak giriş yaptığından burada geçit suçu durumu bulunup bulunmadığının değerlendirilmesi gerekmektedir.[941] Geçitli suç kurumunu kabul eden yazarlar arasında ise görüş

938 Koca ve Üzülmez, a.g.e., s. 815.
"Bilişim sistemine girme suçu bakımından suçun kanuni tanımında açıkça hukuka aykırılık vurgulanmış olduğundan doktrinde bu husus hukuka özel aykırılık olarak adlandırılmaktadır. Hukuka özel aykırılık halinin suç tipinde yer aldığı durumda hâkimin, failin kastı dışında ayrıca bu özel aykırılığı da bilip bilmediğini, buna göre hareket etmeyi isteyip istemediğini de araştırması gerektiği belirtilmektedir." Bkz. Mahmutoğlu, a.g.e., s. 862. Aynı yönde bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7295; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6910.
939 Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", s. 1258.
940 Parlar ve Hatipoğlu, a.g.e., s. 3744.
"…Aşamalarda tanık olarak dinlenen .'nun, katılan şirkete ait siteye yıllık ücretini yatırarak abone olduğu, sanığın tanıktan aldığı kullanıcı adı ve şifre bilgileri ile, tanığın bilgisayarından doğrudan ve TeamViewer isimli program aracılığıyla uzaktan bağlantı yoluyla katılan şirkete ait web sitesine yasal yollardan giriş yaparak site içeriğindeki bazı bilgileri kopyaladığı, kopyalanan bu bilgilerin sanığın çalıştığı şirkete ait internet sitesine konulduğuna dair bilgi olmadığı, dolayısıyla katılan şirkete ait siteye yasal olmayan yollardan giriş yapılmadığı, olayın hukuki nitelikte bulunduğu, TCK'nın 243. maddesinde tanımlanan suçun yasal unsurlarının oluşmadığı gözetilmeden, sanığın beraatı yerine mahkumiyetine karar verilmesi, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 15.6.2015 t., E: 2014/35223, K: 2015/19051, https://legalbank.net/arama, ET. 15 Temmuz 2020.
941 Geçit suçu ise bir suçun işlenmesi için öncelikle cezası daha hafif olan bir suçun işlenmesi, bu suçtan geçilmesinin gerekmesi hali olup işlenen ilk suç ile sonraki daha ağır suçun aynı hukuksal değeri koruması gerekmektedir. Korunan hukuksal değerlerin farklı olması halinde ise ihlal edilen her hukuksal değer açısından eylemler ayrı suç oluşturacağından gerçek içtima kuralları uygulanacaktır. Bkz. Apaydın, "Bilişim Sistemine Girme Suçu", s. 290, 291.

ayrılıkları bulunmakta olup bir görüşe göre, sisteme girip kalmanın araç suç olduğu, girişten sonra amaç suçun gerçekleştirildiğini bu durumda ise sisteme girip kalmanın amaç suçun unsuru ya da cezayı artıran hali olarak düzenlenip düzenlenmediğine bakılarak ceza tayininin gerçekleştirilmesi gerektiğini örneğin sisteme girip kalma TCK'nın 132, 133, 134, 135, 142, 158, 244, 245. m.'lerinde suçun unsurlarından olan icra hareketlerinden sayılmadığından bu durumda faile hem 243. m.'den hem de diğer fiillerden ayrı ayrı ceza verilmesi gerekecek, 243. m. gerçekleştirilmeden amaç suç yapılamıyorsa fail sadece neticeden sorumlu olmalı ve sadece amaç suçtan cezalandırılacaktır.[942] Doktrinde yer alan bir diğer görüşe göre ise, bu durumlarda fikri içtima uygulanarak TCK 124, 132, 244 gibi cezası daha ağır olan suçtan cezalandırılmaya gidilmelidir.[943] Bir başka görüşe göre ise, her somut olay ve hareket

"Bilişim sistemine hukuka aykırı erişim ve sistemde kalmaya devam etme, bilişim sistemlerine girerek işlenmesi zorunlu bulunan başka bilişim suçlarının işlenmesi için bir araçtır. Bu itibarla 243'üncü maddede yer alan suç, daha sonra işlenen bu suçlar bakımından bir geçit olma özelliği taşır ve fail sadece amaç suçtan dolayı cezalandırılır. Örneğin, bir bilişim sisteminin işleyişini engellemek amacıyla bilişim sistemine giren fail, 244'üncü maddeden cezalandırılır. Yine failin hırsızlık (m.142/2(e)) veya dolandırıcılık (m.158/1(f)) suçlarını işlemek kastıyla bilişim sistemine girmesi halinde de, sadece bu son hükümler uygulanır." Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6912, 6913.

942 Bkz. Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1419.

"…bilişim sistemine girme başka suçların işlenmesinde bir araç suç fonksiyonu görebilir. Örneğin fail bir başkasının bilgisayarına onun özel hayatına ilişkin resimlerini veya video filmlerini elde etmek ya da elektronik postalarını okumak amacıyla girebilir. Bu gibi hallerde hem bilişim sistemine girme hem de duruma göre özel hayatın gizliliğini ihlal (m. 134), kişisel verileri hukuka aykırı olarak ele geçirme (m. 136) veya haberleşmenin gizliliğini ihlal (m. 132) suçları oluşacaktır. Amaç suç-araç suç ilişkisinin olduğu hallerde bu suçların icra hareketleri arasında kısmen veya tamamen bir örtüşme yoksa her bir suçtan dolayı failin ayrı ayrı cezalandırılması gerekir. Aksi takdirde failin ceza sorumluluğu farklı neviden fikri içtima hükmüne göre belirlenmelidir.

Bu bağlamda TCK'nın 243. maddesindeki suç ile 244. maddesinde düzenlenen suçlar arasında bir fikri içtima ilişkisinin varlığı kabul edilmelidir. Zira 243. maddede düzenlenen bilişim sistemine girme fiili, bilişim sisteminin işleyişini engelleme veya sistemdeki verilere zarar verme fiilleriyle tamamen örtüşmektedir." Bkz. Koca ve Üzülmez, a.g.e., s. 818, 819.

"Kanaatimizce amaç suç-araç suç ilişkisinde amaçlanan suçun ayrıca işlenmesi halinde gerçek içtima kuralları uygulanmalıdır. Bu bağlamda bilişim sistemine hukuka aykırı olarak girip kalma, TCK' nın 132, 133, 134, 135, 142, 158, 244, 245'inci maddelerinde suçun unsurlarından olan icra hareketlerinden sayılmadığından fail hem TCK m.243 hem de diğer eylemden ayrı ayrı cezalandırılmalıdır." Bkz. Doğan, a.g.e., s. 99, 100.

"Bilişim sistemine girmenin araç suç olarak düzenlendiği veya bilişim sistemine girerek veya bu sistem kullanılarak suçun işlenmesinin suçun unsuru veya nitelikli hal sayıldığı durumlarda, ayrıca faile bilişim sistemine girme suçundan ceza verilemez. Örneğin failin, birisinin bilişim sistemine girerek, bu sistemi bozması halinde yalnızca YTCK'nın 244. maddesindeki suç söz konusu olacak, artık aynı Yasanın 243. maddesi hükümleri uygulanmayacaktır. Yine failin bilişim sistemini aracı kılarak hırsızlık yapması halinde ise sadece YTCK'nın 142/2e, dolandırıcılık yapması halinde ise sadece YTCK'nın 158/1f. maddesi uyarınca cezalandırılacaktır. Ancak, bilişim sistemine girme bir suçun unsuru veya nitelikli hali değilse burada her iki suçtan da ceza verilecektir." Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7301.

Yine Karakehya da aynı yönde olan görüşünde: "…Yani sisteme girme suçun unsuru veya zorunlu davranışı değilse, fail hem bilişim sistemine girmeden hem de amaç suçtan ayrıca cezalandırılacaktır." Ayrıntılı bilgi için bkz. Karakehya, "Türk Ceza Kanununda Bilişim Sistemine Girme Suçu", s. 21, 22.

943 Bkz. Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1419.

açısından değerlendirme yapılması gerekmekte olup geçit suçunun varlığından bahsedebilmek için ilk suçtan geçilmeksizin ikinci suçun işlenememesi gerekmektedir.[944] Kanaatimizce, somut olayın özellikleri ve failin kastı dikkate alınmak suretiyle sisteme girme veya kalma eyleminin suçun unsuru ya da cezayı artıran hali olarak düzenlenip düzenlenmediğine bakılarak çözüme ulaşılması gerekmekte olup bu doğrultuda sisteme girme veya kalma eyleminin (243. m.) suçun unsurlarından olan icra hareketlerinden sayılmadığı hallerde faile hem 243. m.'den hem de diğer suçlardan ayrı ayrı ceza verilmesi, 243. m. gerçekleştirilmeksizin asıl amaçlanan suçun gerçekleştirilemediği hallerde başka bir deyişle ilk suçtan geçilmeksizin ikinci suçun işlenemediği hallerde sadece asıl amaçladığı suçtan cezalandırılmalıdır. Nitekim, Yargıtay' ın da vermiş olduğu kararlar da bu yöndedir.[945] Ancak şunu da belirtmek gerekir ki, nesnelerin interneti teknolojisi ve

Mahmutoğlu ise, 243. maddede düzenlenen suçun, bilişim sistemlerine girilerek işlenmesi zorunlu bulunan başka bilişim suçunun (örneğin 142/2-e hırsızlık ve 158/1-f dolandırıcılık suçlarında) işlenmesi bakımından araç suç niteliğinde olduğu yönünde doktrinde yer alan görüşleri kabul etmeyerek 243. maddede düzenlenen bilişim sistemine girme suçunun 142/2-e hırsızlık ve 158/1-f dolandırıcılık suçlarının nitelikli hali olduğundan bu suçları bileşik suç olarak kabul etmekte ve fail sadece amaç suçtan cezalandırılır görüşüne katılmamaktadır. Bunun yanında yine aynı nedenlerle gerçek içtima kurallarının uygulanması gerektiği fikrini de bu sebeple reddetmektedir. Ancak TCK 136. maddede düzenlenen hukuka aykırı olarak verileri ele geçirme suçu ile 243. maddede düzenlenen bilişim sistemine girme suçunun birlikte işlendiği hallerde ise fikri içtima hükümlerinin uygulanabilme olasılığının bulunduğunu belirtmektedir. Bkz. Mahmutoğlu, a.g.e., s. 864, 865.

944 Dülger' e göre, bilişim sistemlerine hukuka aykırı olarak girilerek gerçekleştirilen 244, 245, 132, 133, 134, 135, 136, 142, 158. maddelerde yer alan bazı suç tiplerinde failin elde etmek istediği amaca yönelik eylemlerini gerçekleştirebilmek için öncelikle üzerinde eylemlerini gerçekleştirebileceği bilişim sistemine hukuka aykırı olarak girmekte olduğundan bunlar arasında geçit suçu durumunun bulunup bulunmadığı sorusunun yanıtlanması gerekecektir. Geçit suçu, bir suçun işlenmesi için öncelikle cezası daha hafif olan bir suçun işlenmesi hali olup işlenen ilk suçun ve sonraki daha ağır suçun aynı hukuksal değeri koruması gerekir. 243. maddede bilişim sisteminin güvenliğini korumakta iken belirtilen maddeler arasında 244. madde dışında farklı hukuksal değerler korunmaktadır. Bu nedenle her somut olay ve hareket açısından değerlendirme yapılması gerekmektedir. Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 299.

945 Yargıtay 12. Ceza Dairesi' nin bir kararında: "Sanığın, katılan ile internette tanıştığı ve bir süre telefonda ve msn üzerinden görüntülü görüşerek arkadaşlık yürüttüğü, sanığın teklifi üzerine katılanın, kendisi, kızı ve sanık ile birlikte bir otelde yaklaşık 1 hafta süreyle tatil yaptıkları, bilahare arkadaşlıklarının bitmesi üzerine, sanığın, katılanın kullandığı elektronik posta adresine rızası dışında birçok kez girerek, arkadaş listesindeki kişilere, değişik zamanlarda başka elektronik posta adresleri üzerinden, katılanın, tatilde deniz kenarında bikini ile güneşlenirken çekilen fotoğrafları, otelde bar ortamında çekilen fotoğrafları, eski erkek arkadaşları ile olan fotoğrafları, msn üzerinden görüntülü görüşme sırasında çekilen çıplak ve yarı çıplak görüntüleri ile web kamera karşısında soyunurken çekilen video görüntüleri gibi özel yaşam alanına ilişkin fotoğraf ve video görüntülerini rızası dışında göndermek suretiyle ifşa ettiği olayda; sanığın, bu şekilde eyleminin TCK'nın 243/1'inci maddesine uyan bilişim sistemine girme suçu ile TCK'nın 134/2'nci maddesine uyan özel hayatın gizliliğini ihlal suçunu oluşturduğu, iddianamedeki anlatımda nazara alındığında, sanığın bu suçlardan sorumlu tutularak cezalandırılması gerektiği gözetilmeden, suçun nitelendirilmesinde yanılgıya düşülerek olayda uygulama yeri bulunmayan TCK'nın 244/2'nci maddesi uyarınca hüküm kurulması,… BOZULMASINA" Yargıtay 12. Ceza Dairesi, 7.7.2014 tarih, E.2013/28897, K.2014/16663, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Aynı yönde bkz. Yargıtay 12. CD., 13.1.2016 t., E:2015/15933, K: 2016/277.

esasen 5G ile birlikte birbirine bağlı çok fazla cihazın bulunacak olması, bilişim ağlarının büyümesi de göz önüne alındığında önümüzdeki günlerde bilişim suçlarının da çeşitlilik kazanacağı belirtilmekte ve bu konuda da çalışmalar yapılması gerektiği vurgulanmaktadır.[946] Klasik anlamdaki suçların birçoğunun bilişim sistemlerinin araç olarak kullanılması suretiyle gerçekleştirilebilmesi mümkün hale gelebilecektir. Böyle bir durumun varlığı göz önünde öngörülü bir düzenleme ile bilişim sistemlerinin araç olarak kullanılmasının sadece hırsızlık ve dolandırıcılık suçuna hasredilmesi yetersiz kalacak olup kanaatimizce öncelikle bilişim alanında suç tipine haiz olan 243. ve 244. m.'lerde yer alan suçların tek bir madde içerisinde farklı fıkralar olarak bir bütün halinde düzenlenmesi bu madde içerisinde de diğer herhangi klasik suç tipi açısından bilişim sistemlerinin araç olarak kullanılmasının genel ağırlaştırıcı sebep olarak kabul edilmesi yerinde bir düzenleme olacaktır.

3.2.1.6. Suçun Nitelikli Halleri

3.2.1.6.1. Bedeli Karşılığı Yararlanılabilen Sistemlere Hukuka Aykırı Olarak Girme veya Kalmaya Devam Etme (TCK madde 243/2)

243. m.'nin 2. fıkrasında bilişim sistemine girme suçunun daha az cezayı gerektiren nitelikli hali düzenlenmiş olup buna göre failin bedelini ödeyerek hukuka uygun olarak girebileceği bir bilişim sistemine bedel ödemeksizin girmesi veya orada kalmaya devam etmesi halinde suçun temel cezası yarı oranında indirilerek verilecektir.[947] "Bedeli karşılığında yararlanılabilen sistem" ifadesi bilişim alanında suçlar arasında ilk defa düzenlenmiş olmasına rağmen kanunda veya gerekçesinde kavrama ilişkin bir açıklama yapılmamıştır.[948] Biz az önce de belirtmiş olduğumuz üzere bu kavramın, bedelini ödeyerek hukuka uygun olarak girebilecek ve içerdiği veri veya hizmetlerden yararlanılabilecek olan bir bilişim sistemi olarak değerlendiriyoruz. Bu bağlamda, elektronik arşiv merkezleri, elektronik gazeteler, alışveriş siteleri gibi internet üzerinden ücret karşılığı hizmet veren web siteleri[949] bu sistemlere en iyi örnekleri oluşturmaktadır.[950] Elektronik yapıda bulunan hizmetin bedeli karşılığında

946 Sağıroğlu, a.g.e., s. 48.
947 Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", s. 1396; Yaşar, Gökcan, Artuç, a.g.e., s. 7299.
948 Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", s. 1396; Artuk, Gökcen ve Yenidünya, Türk Ceza Kanunu Şerhi: Madde 234-345, s. 6908.
949 Yaşar, Gökcan ve Artuç, a.g.e., s. 144.
950 "Bedeli karşılığı yararlanılabilen sistem kavramının, herkesin girmesinin mümkün olmadığı, ancak belli süreler için öngörülen bedel ödendiği takdirde, genellikle müşteriye verilen şifre ile girilebilen sistemler olarak anlaşılması gerekir." Bkz. Parlar ve Hatipoğlu, a.g.e., s. 3746.

elde edilmesi yaptırıma bağlandığından bedeli karşılığı bilişim sistemini kiralayan internet cafe vb. yerleri ise fıkra kapsamında değerlendirmiyoruz.[951] Decoderlerin bedeli karşılığında yararlanılabilen sistemlerden olup olmadığı[952] ve yayınların izlenmesi halinde suçun TCK' nın 163/2. m.'sinin mi yoksa 243/2. m.'si kapsamında mı değerlendirileceği hususunda ise kanaatimizce doktrinde yer alan benzer görüşlerde de belirtildiği üzere şifreli yayınları alan, bu şifreyi çözdükten sonra işleme tabi tutarak çıkarmış olduğu veriyi alıcıya gönderebilen decoderler bilişim sistemi ve madde kapsamında bedeli karşılığında yararlanılabilen sistem olarak kabul edilebilecek ancak TCK' nın 163. m.'sinin 2. fıkrasına göre "telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan" kişi, fiile ilişkin özel düzenleme bulunması sebebiyle TCK 243/2. m. kapsamında değil, TCK 163. m.'sinde yer alan karşılıksız yararlanma suçundan cezalandırılacaktır.[953]

---

951 Benzer yönde bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 143, 144; Parlar ve Hatipoğlu, a.g.e., s. 3746; Mahmutoğlu, a.g.e., s. 863;
Erdoğan' a göre, "…Bizimde katıldığımız ikinci grupta yer alan yazarlar ise; burada kastedilenin bilişim sisteminin kullanıldığı mekanın değil, bizzat bu sistem içerisindeki elektronik yapıda sunulan ücretli hizmetlerin olduğunu, bu nedenle, internet kafedeki bilgisayarların ücretsiz kullanılmasının ya da belli süreli internet bağlantı servisinin sağlanmasının bu fıkra kapsamında olmadığını belirtirler." Bkz. Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1399.
Aksi yönde görüş için bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7299;
" …,bedeli karşılığı yararlanılabilen sistem kavramından, bugün için internet üzerinden ücret karşılığı hizmet veren web siteleri, belirli bir bedel karşılığı bilişim sistemi kiralayan yerlerdeki bilişim sistemleri (örneğin, internet kafeler) anlaşılır.
…bedeli karşılığı yararlanılabilen sistem kavramından; a) manuel olarak müdahale edilerek bedel karşılığı girilen bilişim sistemlerini, b) ağ vasıtasıyla ulaşılan bilişim sistemlerini anlıyoruz…" Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6909.
"İnternet üzerinden ücret karşılığı hizmet veren web sitesine, internet kafelerde bulunan ücret karşılığı yararlanılabilen sisteme, bedeli karşılığı internet bağlantılı servisi sağlayan sistemlere girilmesi şdurumunda cezada yarı oranına kadar indirim yapılacaktır." Bkz. Gül, a.g.e., s. 68.
952 "Şifreli yayınların izlenmesinde kullanılan dekoder (şifre çözücü) isimli cihazların, bilgileri otomatik işleme tabi tutmuş sistem kavramı içinde değerlendirilip değerlendirilemeyeceği ise, önceki TCK döneminde ülkemizdeki yoğun tartışma konularından birini oluşturmuştur.
Bu konuda doktrinde ve uygulamada baskın olan görüş, dekoderin bilgisayar kapsamında olmadığı ve bu sebeple de, bu cihaz aracılığı ile gerçekleştirilen eylemlerin eski TCK'nın 11. bab hükümlerine göre değerlendirilemeyeceği yönündeydi. Bizim kanaatimiz de bu yöndedir.
… Ancak ceza hukukumuzda bu konuda bir ihtiyaç olduğu açıktı. Bu sebeple kanunkoyucu yeni TCK'da bu konuda açık bir düzenleme öngörmüştür. Ancak düzenleme yukarıda belirttiğimiz nedenlere bağlı olarak bilişim alanında suçlar başlığı altında değil; faydalanma suçuna ilişkin olarak getirilmiştir. Dolayısıyla söz konusu fiilleri işleyen kimselerin, artık karşılıksız faydalanma suçu kapsamında cezai sorumlulukları doğacaktır." Karakehya, "Türk Ceza Kanununda Bilişim Sistemine Girme Suçu", s. 9, 10.
Ayrıntılı bilgi için bkz. Yazıcıoğlu, "Şifreli Yayınların Bilişim Suçları Karşısındaki Konumu", s. 47-69.
953 Benzer yönde bkz. Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1398; Yaşar, Gökcan ve Artuç, a.g.e., s. 7299; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6909; Mahmutoğlu, a.g.e., s. 863;
Akbulut' a göre de: "…son yıllarda kullanılan TV yayınlarında IP tekniği kullanıldığından bilişim sistemi içerisinde nitelendirilebilecek özelliğe sahiptirler. Dolayısıyla ücretli olan şifreli yayınların

243. m.'nin 2. fıkrası düzenlemesinde öngörülen hafifletici sebebin yerinde olup olmadığı konusunda da doktrinde farklı görüşler bulunmakta olup Erdoğan' ın da savunduğu görüşe göre, bu suçla korunan hukuksal değerler arasında sistem sahibinin menfaatleri de güvence altına alındığından bu indirimin yerinde olmadığıdır.[954] Yine Özbek ve diğerlerine göre bu suç ile bilişim sisteminin güvenliği yanında o sistemin sadece yetkilendirilen kişilere açık olması sebebiyle veri mülkiyetinin veya zilyetliğin korunması amaçlandığından böyle bir indirim nedeni isabetsizdir.[955] Yine Dülger de söz konusu fıkra düzenlemesi ile iki farklı hukuksal değerin ihlali söz konusu olduğundan bunun cezayı ağırlaştıran nitelikli hal olarak düzenlenmesi yerine hafifletici neden olarak düzenlenmesini bir hata olarak değerlendirmektedir.[956] Düzenlemeyi yerinde bulan yazarlara[957] bakıldığında ise, Yaşar ve diğerleri, birinci

internet ağları aracılığıyla şifrelerin kırılması suretiyle izlenmesi durumunda bedeli karşılığı yararlanılabilen bilişim sistemler söz konusu olup, TCK m. 243/2 çerçevesinde cezalandırılmalıdır. Eğer yayınların alınması telefon hatlarıyla veya frekanslarıyla veya elektromanyetik dalgalarla yapılan yayınlardan yararlanma niteliğindeyse o zaman TCK m. 163 kapsamına giren bir durum gerçekleşecektir." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 147.

954 Erdoğan ayrıca şu hususa dikkat çekmiştir: "Ayrıca belirtmeliyiz ki, kanaatimizce, bedel karşılığı olup olmadığına bakılmayıp, sadece kamu kurumları bilişim sistemlerine yapılacak girişlerin cezası ile özel hukuk tüzel kişileriyle gerçek kişilerin bilişim sistemlerine yapılacak girişlerde cezada farklılaşmaya gidilmeliydi." Bkz. Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1400.

Yine Apaydın' a göre de: "…Kanaatimizce de kamu kurumlarının bilişim sistemlerine hukuka aykırı olarak girmenin cezası, özel hukuk tüzel kişileri ile gerçek kişilerin bilişim sistemlerine hukuka aykırı olarak girme fiillerine göre fazla olmalıdır." Bkz. Apaydın, "Bilişim Sistemine Girme Suçu", s. 272.

955 Zira, bu durumun kabulü halinde bedeli ödenmeden o sistemin kullanılıyor olmasından ötürü bilişim sistemi işleticisi ve onun sistem üzerindeki hakları ihlal edilmiş olacaktır ki bu da düzenleme bakımından bir çelişkiye neden olacaktır. Bkz. Özbek, v.d., a.g.e., s. 926.

956 "243. maddenin 2. fıkrasında belirtilen nitelikli halin gerçekleşmesi halinde hem suçun basit halindeki sistem güvenliği hukuksal değeri ihlal edilmiş olacak hem de bedeli karşılığı girilebilen bir sistemin güvenliği ihlal edildiği için, bir şekilde sistemin sahibi ya da ilgilisinin malvarlığının korunmasına yönelik hukuksal değer de ihlal edilmiş olacaktır...

Sonuç olarak belirtilmelidir ki; bu hafifletici neden yerinde bir düzenleme değildir. Bu fıkranın hangi sistemlere uygulanacağına dair ne yasa metninde ne de yasanın gerekçesinde bir açıklama bulunmamaktadır…Kısaca cezanın hafifletilmesini sağlayacak yönde ne failin kastında ne de korunan hukuksal değerlerde bir azalma bulunmamakta, aksine artış bulunmaktadır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 269, 272.

Akbulut' a göre ise TCK'nın 116/2. fıkrasında olduğu gibi girilen yerin bazı sistemler olması cezada indirim yapılmasını gerektiren bir hal olarak kabul edilecekse de bu suçta konut dokunulmazlığını ihlal suçundan farklı olarak ekonomik yarar sağlanması söz konusu olduğundan sisteme girme açısından kabul edilebilecek olan bazı sistemlere girişin cezanın daha az verilmesini gerektiren nitelikli hal olarak düzenlenmesi sistemde kalmaya devam etme açısından kabul edilemeyecektir. Bu kapsamda, ikinci fıkra bağımsız bir suç haline getirilmeli, karşılıksız yararlanma suçu kapsamında bilişim sistemleriyle ilgili ayrıca belirleme yapılmalı ya da 244. maddenin 1. ve 2. fıkralarındaki düzenlemeleri de kapsayacak şekilde ancak sadece bu fıkralarla sınırlı kalmayacak şekilde bilişim sistemleri aracılığıyla yarar sağlama suçuna ilişkin düzenleme yapılmalıdır. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 143.

957 Bkz. Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", s. 1259; Mahmutoğlu, a.g.e., s. 863;

Apaydın' a göre: "…Bu hükmün getiriliş amacı özel kişilere ait bir bilişim sistemine girmek ve orada kalmak halinde ihlal edilen hukuki yararın, bedeli karşılığında yararlanılan sistemlere girmek

fıkrada yer alan suçun bilişim sisteminin güvenliği ve özel hayatın gizliliği hukuksal menfaati korumakta iken ikinci fıkrada bu yararın malvarlığının korunmasına doğru kayması sebebiyle indirim öngörüldüğünü belirtmekte[958] iken Artuk ve diğerlerine göre bilişim sistemine hukuka aykırı erişim suçu, sistemin güvenliği ve bireylerin mahremiyeti hukuksal değerlerini korumakla beraber hak sahibinin ücreti karşılığında erişime izin vermesi halinde korunan hukuksal değerlerden mahremiyetin yerini ekonomik menfaate bırakması sebebiyle yasa koyucu tarafından daha az bir yaptırım öngörülmüştür.[959] Koca ve Üzülmez' e göre ise hak sahibinin bedeli ödendiği takdirde sisteme girilmesine izin vermesi ile bedeli ödeyenler bakımından sistemin güvenliğinden sarfı nazar ettiği bu şekilde girilen bir sisteme müdahalenin haksızlık içeriğinin ise hiçbir şekilde girilmesine izin verilmeyen sisteme nazaran çok daha az olması sebebiyle cezada indirim öngören düzenleme isabetlidir.[960] Doğan' a göre de, ticari bir gaye ile belli bir bedel karşılığında 3. kişilere sunulan verilerin masumiyeti ile hiçbir şekilde kullanım ve erişim izni verilmeyen verilerin masumiyeti arasında fark bulunmakta olup 2. fıkrada malvarlığı, 1. fıkrada ise bilişim sisteminin güvenliği ve özel hayatın korunması olduğundan 2. fıkrada meydana gelen tehlikenin 1. fıkraya göre daha az olması sebebiyle de bu düzenleme yerinde bir düzenlemedir.[961]

Kanaatimizce de bu düzenleme yerinde bir düzenlemedir. Zira, 243. m.'sinin birinci fıkrasında düzenlenen suçun temel şeklinin koruduğu hukuksal yararın karma nitelikte olduğunu ancak esasen bilişim sisteminin güvenliği ve güvenilirliğinin korunmak istendiğini belirtmiştik. Kanun koyucunun burada 3. kişilerin girişine tamamen kapalı bir sisteme hukuka aykırı girme veya kalma eylemi sonucunda toplumun tamamının karşılaşacağı tehlikenin, bedeli alınmak suretiyle yararlanılmasına veya girilmesine izin verilen başka bir deyişle bir şekilde 3. kişilerin erişimine açılan bir sisteme hukuka aykırı girme veya kalma halinde karşılaşılacak tehlikeye nazaran daha fazla olduğunu değerlendirerek düzenleme yaptığını düşünmekteyiz. Bu anlamda, maddenin düzenlenmiş olduğu bilişim alanında suçlar bölümünün topluma karşı suçlar kısmında düzenlendiği de dikkate alındığında, Doğan' ın da belirtmiş olduğu gibi 2. fıkrada düzenlenen nitelikli halin koruduğu

ve orada kalmak suretiyle ihlal edilen hukuki yarardan daha fazla korunmaya değer olduğu düşüncesine dayandırılmaktadır." Bkz. Apaydın, "Bilişim Sistemine Girme Suçu", s. 272.
958 Yaşar, Gökcan ve Artuç, a.g.e., s. 7298, 7299.
959 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6908.
960 Koca ve Üzülmez, a.g.e., s. 816.
961 Doğan, a.g.e., s. 80.

hukuksal değerin malvarlığının korunmasına yönelmesinin suçun esas şekline göre daha az ceza ile cezalandırılması yerinde bir düzenlemedir.

3.2.1.6.2. Suçun Terör Amacıyla ve Terör Örgütünün Faaliyeti Çerçevesinde İşlenmesi

3713 sayılı Terörle Mücadele Kanunu' nun 4. m.'si[962] uyarınca 5237 sayılı TCK' nın "Bilişim Alanında Suçlar" bölümünde yer alan 243 ve 244. m.'lerindeki suçların TMK' nın 1. m.'sinde belirtilen terör amacıyla, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlenmesi halinde terör suçu sayılacağı belirtilmiş olup aynı Kanun' un 5. m.'sinde ise söz konusu suçların (3. ve 4. m.) terör amacıyla işlenmesi halinde ilgili kanunlara göre tayin edilecek hapis cezaları veya adli para cezalarının yarı oranında artırılarak hükmolunacağı, bu suretle tayin olunacak cezalarda o fiil için ve her nevi ceza için muayyen olan cezanın yukarı sınırının aşılabileceği ayrıca bu madde hükümlerinin çocuklar hakkında uygulanmayacağı belirtilmiştir.[963]

3.2.1.7. Suçun Neticesi Sebebiyle Ağırlaşmış Hali (TCK madde 243/3)

243. m.' nin 3. fıkrasında, 1. fıkrada yer alan bir bilişim sisteminin bütününe veya bir kısmına kasten ve hukuka aykırı olarak girme veya kalmaya devam etme fiili sonucunda "sistemin içeriğinin değişmesi veya yok olması" söz konusu olup doktrinde farklı değerlendirmeler mevcut ise de madde gerekçesinde bu durum "üçüncü fıkrada, bu suçun neticesi sebebiyle ağırlaşmış hali düzenlenmiştir" şeklinde belirtilmiştir.[964] Biz de 3. fıkra düzenlemesinin bilişim sistemine girme suçunun neticesi sebebiyle ağırlaşmış hali olarak kabul ettiğimizden bu başlık içerisinde incelemekteyiz.[965] Bir

962 "Madde 4 –(Değişik: 29/6/2006-5532/3 md.)Aşağıdaki suçlar 1 inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır:a) Türk Ceza Kanununun 79, 80, 81, 82, 84, 86, 87, 96, 106, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 142, 148, 149, 151, 152, 170, 172, 173, 174, 185, 188, 199, 200, 202, 204, 210, 213, 214, 215, 223, 224, 243, 244, 265, 294, 300, 316, 317, 318 ve 319 uncu maddeleri ile 310 uncu maddesinin ikinci fıkrasında yer alan suçlar…" bkz. https://mevzuat.gov.tr/mevzuatmetin/1.5.3713.pdf 23, ET. Mart 2010.

963 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 274; Akbulut, *Bilişim Alanında Suçlar*, s. 208.

964 A.e., s. 264.

965 Aynı yönde görüş için bkz. Apaydın, "Bilişim Sistemine Girme Suçu", s. 274; Koca, Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 817; Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", s. 1259; Mahmutoğlu, a.g.e., s. 863; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6911; Yaşar, Gökcan ve Artuç, a.g.e., s. 7297.
Özbek vd.' ne göre: "Daha önce de ifade edildiği üzere, öğretide bu hükmün bir nitelikli hal olarak değerlendirilmesi gerektiği yönünde görüşlere rastlamak mümkünse de, TCK m. 243/3 münferit bir

suçun neticesi sebebiyle ağırlaşmış suç olarak kabulü için bir fiilin, kastedilenden daha ağır veya başka bir neticenin oluşumuna sebebiyet vermesi halinde failin bundan sorumlu tutulabilmesi için bu netice bakımından en azından taksirle hareket etmesi gerekmekte olduğundan 243. m.'nin 3. fıkrası kapsamında failin de en azından taksirle hareket etmesi zorunludur.[966] Başka bir anlatımla, verileri yok etmek veya değiştirmek failin kastı kapsamında yer almamalı, gerçekleşen bu sonuç failin taksiri sonucunda gerçekleşmelidir.[967] O halde, failin olası veya doğrudan kastının ağır neticeye (verileri yok etmek veya değiştirmek) yönelmesi halinde TCK 244/2. m.'de yer alan suç oluşacağından böyle bir durumun varlığı halinde 243/3. m. uygulama alanı bulamayacaktır.[968]

3.2.1.8. Kusurluluk

Söz konusu suç tipi kusurluluk açısından ayrı bir özellik arz etmemektedir.

3.2.1.9. Veri Nakillerini Sisteme Girmeksizin Teknik Araçla İzleme Suçu (TCK madde 243/4)

24.3.2016 tarihli ve 6698 sayılı "Kişisel Verilerin Korunması Kanunu"nun 30. m.'sinin 4. fıkrası ile TCK'nın 243. m.'sine 4. fıkrasında: *"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."*[969] şeklinde düzenlenen suç tipi AKSS' nin "yasadışı araya girme" başlıklı 3. m.'sinde taraf devletlere getirilen yükümlülüğün karşılanması amacıyla

suç olarak, daha özel bir ifadeyle neticesi sebebiyle ağırlaşmış bir suç olarak kabul etmek gerekmektedir. Çünkü cezai müeyyide altına alınan hareket tek başına bilişim sistemine girme ve orda kalma değil, bu hareket dolayısıyla sistemde yer alan bir verinin yok edilmesi veya değiştirilmesidir." Bkz. Özbek, v.d., a.g.e., s. 925.
Akbulut da: "…TCK m. 243/3'de yer alan düzenlemenin nitelikli hal olduğu değerlendirmesi doğru değildir. Birincisi, 3. fıkradaki neticenin taksirli olarak gerçekleştirilmesi gerektiği için, nitelikli haller de kastın kapsamında olduğu ve bilinmesi gerektiği için, nitelikli haller taksirli olarak gerçekleştirilemez. İkincisi nitelikli şeklinde temel suç tipinde yer almayan bir neticenin gerçekleştirilmesi söz konusu değildir (TCK m. 243/1). Ama aynı maddenin 3. fıkrasında bir neticenin gerçekleşmesi aranmaktadır. Bağımsız suç olması da söz konusu değildir. Ayrı bir fiille gerçekleştirilen ve kendine ait unsurları olan bir fiil değildir. Dolayısıyla biz de doktrinin çoğunluğuna katılarak TCK m. 243/3'de yer alan düzenlemenin bilişim sistemine girme suçunun netice sebebiyle ağırlaşmış şekli olduğunu benimsiyoruz." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 148, 149.
966 Özbek, v.d., a.g.e., s. 925.
967 Apaydın, "Bilişim Sistemine Girme Suçu", s. 274.
968 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 266; Akbulut, *Bilişim Alanında Suçlar*, s. 149; Parlar ve Hatipoğlu, a.g.e., s. 3746, 3747.
969 Koca ve Üzülmez, a.g.e., s. 820.

mevzuatımıza bağımsız bir suç tipi olarak dahil edilmiştir.[970] Düzenlenen suç tipi ile yasaklanan eylem, verilere müdahale edilmesi değil, verilerin bir bilişim sisteminden diğer bir bilişim sistemine nakli sırasında teknik araçlarla izlenmesi[971] olup bilişim teknolojilerinde yaşanan gelişmelerle sisteme girilmeden de verilere ulaşılması söz konusu mümkün hale geldiğinden AKKS'nin getirmiş olduğu yükümlülüğe de uygun olarak yapılan yerinde düzenlemenin söz konusu suç tipi Ceza Kanunumuz bakımından bir boşluğu doldurduğu söylenebilmektedir.[972] Ancak bizim de katılmış olduğumuz üzere, doktrinde söz konusu suç tipinin düzenlenmiş olduğu yerin (243. m.'nin 4. fıkrası) hatalı olduğu, madde başlığı ile uyumlu olmadığı ve ayrı bir m. (243/A) olarak düzenlenmesinin yasa yapma tekniği açısından uygun olacağı belirtilmektedir.[973]

970 Akbulut, *Bilişim Alanında Suçlar,* s. 157.
"Hükümler karşılaştırıldığında TCK m. 243/4 verilerin izlenmesini Sözleşme ise araya girme ifadesini kullanmıştır. Sözleşme umuma kapalı olarak iletilmesini ve sisteme girmeksizin izlenmesini ararken düzenlememizde böyle bir belirleme bulunmamaktadır. Diğer bir fark da elektromanyetik dalgalarla yayılma ifadesinin TCK m. 243/4'te kullanılmamasıdır. Bunların dışında düzenlemelerin aynı olduğu görülmektedir. Sözleşmede şarta bağlanabileceği ifade edilmişse de buna ilişkin hükme fıkrada yer verilmemiştir." Bkz. A.e., s. 158.
"Siber Suçlar Sözleşmesi'nin "araya girmenin" geniş biçimdeki yorumunu desteklediği görülebilir; bundan dolayı Sözleşme "bir bilişim sisteminden kaynaklanan elektromanyetik yayımları" da araya girmenin bir türü olarak içermektedir. Hatta bu tür teknikler, casus dinleme cihazlarına (böceklere) benzer şekilde, gizli dinlemenin sofistike bir yöntemi biçiminde kolaylıkla kullanılabilir.
TCK ile Sözleşmenin düzenlemeleri karşılaştırıldığında, sözleşmedeki umuma (kamuya) kapalı olarak iletme ve elektronik dalgalarla yayımla ifadelerinin 243/4'te bulunmadığı görülür. Dolayısıyla TCK'da, Sözleşmeye göre daha kapsamlı bir düzenleme yapılmıştır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 304.
971 "Bu tür fiiller bazı işleniş şekilleri itibariyle TCK'da düzenlenen haberleşmenin engellenmesi (m. 124), haberleşmenin gizliliğini ihlal (m. 132), özel hayatın gizliliğini ihlal (m. 134) suçlarıyla örtüşebilir. Ancak uygulamada bu suçların tanımına girmeyen durumlarla da karşılaşılabilir." Bkz. Koca ve Üzülmez, a.g.e., s. 820.
"Mevcut düzenlemeler bu tür eylemleri karşılamada yetersiz kalmaktadır. TCK'nın 132. maddesi haberleşmenin gizliliğini, TCK'nın 135. maddesi kişisel verilerin kaydedilmesini, TCK m. 136 kişisel verilerin ele geçirilmesini 243/1, bilişim sistemine girmeyi cezalandırmaktadır. Bu düzenlemeler (sadece kişisel veri olması, sisteme girmeyi araması, tedbir almayı gerektirmesi veya ağları kapsamaması nedeniyle) bilişim teknolojisinin oratya çıkardığı gelişmeler çerçevesinde bir bilişim sisteminden diğer bir bilişim sistemine veri nakil ağlarıyla verilerin nakledildiği sırada bunların izlenmesini karşılayacak nitelikte değildi. Buna ilişkin bir düzenlemeye ihtiyaç bulunmaktaydı. Ayrıca bugün kablosuz internet erişiminde verilerin şifrelenmesinin kullanılmasının hala yaygın olmaması da bu gereksinimi ortaya çıkarmaktadır. Kanun koyucu da TCK m. 243/4' eklediği hükümle bu ihtiyacı ortadan kaldırmıştır." Bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 158.
972 Koca ve Üzülmez, a.g.e., s. 820; Akbulut, *Bilişim Alanında Suçlar,* s. 158.
"…Özellikle bluetooth, wifi vb.gibi kablosuz iletişim araçlarının yaygınlaşması ile günümüzde veri aktarımlarının çoğu bu yollarla yapılır hale gelmiştir. Ancak bu yöntemlerle yapılan aktarımların araya girilmesi suretiyle elde edilmesi halinde sisteme girme söz konusu olmadığı için, bu haksızlıklar cezasız kalmaktadır. İşte bu tür haksızlıkları yaptırım altına almak için söz konusu suç tipi düzenlenmiştir. Dolayısıyla bu olması gereken son derece yerinde bir düzenlemedir." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 304.
973 Akbulut, *Bilişim Alanında Suçlar*, s. 158, 159; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 302.

3.2.1.9.1. Korunan Hukuksal Değer

Doktrinde, söz konusu suçla korunmak istenen hukuksal değerin veri iletişiminin gizliliği ve verilerin güvenliği olduğu üzerinde yoğunlaşıldığı görülmektedir. Buna göre, verilerin nakli sırasında teknik araçlarla izlenmesi, verilerin kaynağının ve içeriğinin öğrenilmesi tehlikesi doğurduğundan yasa koyucu, veri nakil ağları ve veri iletişimi yapan kişilerin iletişimini başkalarının gözetiminden uzak şekilde yapmalarını sağlamak istemiş, bu doğrultuda Anayasa ile güvence altına alınmış olan "haberleşmenin gizliliği" genel hakkını koruma altına almıştır.[974] Bu suç ile korunan hukuksal değerin, verilerin güvenliği olduğunu belirten Dülger ise, her ne kadar bilişim sistemleri arası veri aktarımı geniş anlamda sistemin bir parçası olsa da bu suç tipinde açıkça "sisteme girilmeksizin" şartı arandığı için korunan öncelikli değerin sistem güvenliği olmadığını, verinisn ilgilisinin sistemler arasında aktarılan verinin güvenli olmasından kaynaklanan çıkarı olduğunu belirtmektedir.[975] Kanaatimizce, bilişim alanında suçların koruduğu ortak hukuksal değer bilişim sisteminin güvenliği ve güvenilirliği olsa da, Dülgeri' in de belirtmiş olduğu üzere incelemekte olduğumuz suç tipinde bilişim sistemine girilmesi şartı aranmayıp aktarılan verilerin izlenmesi eylemi yaptırıma bağlandığından burada korunan hukuksal değer öncelikli olarak veri iletişiminin gizliliği, faiillerin suç tipinde belirlenmiş olan fiilleri gerçekleştirmesi ile de verilerin içeriğine ulaşma tehlikesi bulunduğundan ikincil olarak veri güvenliğidir. Zira, bu suç tipi ile salt verilerin izlenmesi fiilleri suç olarak düzenlenmiş olup verinin içeriğine ulaşma şartı aranmamaktadır. Bunun yanında, toplumu ilgilendiren suçlar kısmında yer alan "bilişim alanında suçlar" başlığı altında düzenlenen bu suç tipi bir yönü ile de muhakkaktır ki toplumu ilgilendirmektedir. Zira, aşağıda yer alan başlıkta da belirteceğimiz üzere, nakledilen verilerin kamu kurum veya kuruluşuna ait olması halinde toplumu oluşturan bireylerin hepsi esasen mağdur sıfatını taşımaktadır.[976]

974 Koca ve Üzülmez, a.g.e., s. 821; Akbulut, *Bilişim Alanında Suçlar,* s. 159.
975 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 304.
"Bilişim sisteminin bütünlüğe ilişkin suçlar, bir saldırgan tarafından erişilen veya değiştirilen sistemde bulunan "durağan" verilere yöneliktirler. Buna karşın ceza hukuku, ağlar arasında aktarım halinde bulunan ve üçüncü kişiler tarafından araya girilerek etkide bulunulan verileri de korumalıdır. Aktarım halindeki verilere karşı yapılan saldırılarla, sistem içinde bulunan verilere karşı yapılan saldırılarda güdülen amaç aynı olabilir; bunlar, örneğin gizliliğe ve bütünlüğe zarar verilmesi veya verilere erişimin engellenmesi olabilir; ancak birincil zarar geleneksel olarak doğasında bulunan gizliliğin ve mahremiyetin ihlal edilmesidir. Nitekim bu maddenin getirilme nedeni olan Avrupa Siber Suçlar Söz leşmesinin açıklayıcı memorandumunda da bu husus "Bu hüküm veri iletişiminin mahremiyetini korumayı amaçlamaktadır." şeklinde ifade edilmiştir." Bkz. A.e., s. 302, 303.
976 Koca ve Üzülmez, a.g.e., s. 821; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 305.

3.2.1.9.2. Maddi Unsur

3.2.1.9.2.1. Fail ve Mağdur

İncelenmekte olan suç tipinde fail için ayrıca bir özellik aranmadığından herkes bu suçun faili olabilir.[977] Mağdur ise nakledilen veriler üzerinde tasarruf yetkisine göre belirlenmekte olup tüzel kişilerin suçun mağduru olmaları mümkün olmadığından nakledilen verilerin tüzel kişiliğe ait olması halinde tüzel kişiliği oluşturan gerçek kişiler mağdur, tüzel kişilik ise suçtan zarar gören konumunda olacaktır.[978] İzlenen verinin bir kamu kurum ve kuruluşuna ait olması halinde ise, toplumu oluşturan herkes suçun mağduru olacaktır.[979]

3.2.1.9.2.2. Suçun Konusu

243. m.'nin 4. fıkrasında düzenlenen suçun konusu, bilişim sistemleri arasında veya bilişim sisteminin kendi içinde "nakledilen"[980] (aktarılan/iletilen) kişisel veya kişisel olmayan veriler olup nakil halinde olmayan (sabit) veriler suçun konusunu oluşturmamaktadır.[981] Veri nakli sağlayan bağlantının kablolu ya da kablosuz olması internet veya başka özel ağlar olması arasında fark bulunmadığı gibi AKSS' de belirtildiği gibi açıkça belirtilmese de elektromanyetik dalgalar aracılığıyla gerçekleştirilen veri nakilleri de bu suç kapsamına girecektir.[982] Bunun dışında AKKS' nin 3. m.'sinde umuma kapalı iletim ifadesi kullanılmışsa da 243/4 düzenlemesinde veri naklinin üçüncü kişilere açık veya kapalı olmasına ilişkin bir açıklık bulunmamaktadır.[983] Ancak doktrinde madde düzenlemesinde izlemenin hukuka aykırı olması gerektiği belirtildiğinden ve açık veri naklinde ise hukuka aykırılık gerçekleşmeyeceğinden, veri naklinin üçüncü kişilere kapalı olması gerektiği hususunda fikir birliği bulunduğu söylenebilmektedir.[984]

977 Koca ve Üzülmez, a.g.e., s. 821.
978 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 305; Akbulut, *Bilişim Alanında Suçlar*, s. 161.
979 Koca ve Üzülmez, a.g.e., s. 821; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 305; Akbulut, *Bilişim Alanında Suçlar*, s. 161.
980 Veri iletimini sağlayan aracın bilişim sistemi olması koşulu ile e-mail, telefon, telefaks, sohbet odalarında yapılan görüşmeler (chat), VPN, internet üzerinden yapılan görüntülü ya da yalnızca sesli telefon görüşmesi (internet telefonu) gibi yazılım yollu tüm yöntemler geçerli olarak kabul edilecektir. Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 305; Akbulut, *Bilişim Alanında Suçlar*, s. 162.
981 Koca ve Üzülmez, a.g.e., s. 821; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 305; Akbulut, *Bilişim Alanında Suçlar*, s. 161, 162.
982 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 306; Akbulut, *Bilişim Alanında Suçlar*, s. 162.
983 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 306.
984 A.e.; Koca ve Üzülmez, a.g.e., s. 821.

3.2.1.9.2.3. Fiil

243. m.'nin 4. fıkrasında düzenlenmiş olan suçun oluşabilmesi için, bilişim sistemine girilmeksizin "nakledilen"[985] verinin "teknik araçlar"[986]la "izlenme"[987]si gerekmektedir. Söz konusu suç, teknik araçlarla izleme hareketinin yapıldığı anda gerçekleşmekte olup ayrıca bir netice aranmadığından sırf hareket ve soyut tehlike suçudur.[988] Bu bağlamda, suç tipinde suçun oluşumu için verilerin içeriğinin öğrenilmesi (içeriğe vakıf olunması) veya temin edilmesi gerekmemektedir. Bilişim sistemine girmeksizin veri nakillerinin izlenmesi esnasında verilerin içeriğine de vakıf olunması halinde ise kanaatimizce başka suçların da oluşacağı açık olup içtima kuralları uyarınca tek fiilin var olup olmadığına bakılarak hareket edilmelidir. Bu doğrultuda, fail eğer veri nakillerini teknik araçla izleme esnasında ayrıca bir fiil gerçekleştirmeden içeriğe de vakıf oluyor ise bu durumda tek bir fiil ile 243/4. m. yanında haberleşmenin gizliliğini ihlal, özel hayatın gizliliğini ihlal ve verilerin ele geçirilmesi suçları da gerçekleşmiş olacağından TCK m. 44 uyarınca fail en ağır cezayı içeren suçtan cezalandırılacaktır.[989] Ancak failin verilerin nakli sırasında teknik

"…Kamuya açık olmamayla verilerin içeriğinin kamuya kapalı olması kastedilmemektedir. Nakletmenin kamuya kapalı olması ifade edilmektedir. Kanunumuzda kamuya kapalı olmayla ilgili bir belirleme yoksa da suçun oluşması için veri nakillerinin kamuya kapalı olması gerekir…internet üzerinden şifrelenmemiş verilerin nakledilmesinin de kamuya açık olmaması gerekir. Veriler şifrelenmişse kamuya açık olmayan bir nakil olduğu anlaşılmaktadır. Ama hükmün kapsamına girmesi için verilerin şifreli olup olmaması değil iletimin kamuya kapalı olup olmaması değer taşımaktadır. Veri naklinin kamuya kapalı olduğunun söylenebilmesi için verilerin nakledilmesinin nakletmenin amacına göre umuma değil de sınırlandırılmış alıcı çevresine yönelik olmalıdır…İnternetteki haberler ise serbestçe erişilebilir olarak gönderildiği için kamuya açık veri nakli söz konusudur." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 163, 164.

985 "…izleme mutlaka verinin nakledildiği sırada, yani kaynağından çıktıktan sonra ve hedefine ulaşmadan önce, yani yolda gerçekleştirilmelidir." Bkz. Koca ve Üzülmez, a.g.e., s. 822.

986 "Teknik araçlar, hatlar veya elektromanyetik dalgalarla iletilen verilerin izlenmesine imkân veren her türlü teknik cihazı ifade etmektedir. Cihazların yanında programlar, şifreler, kodlar da dâhildir. Örneğin ağ üzerindeki veri trafiğini izlemeye yarayan sniffing yöntemi, wireshark isimli program verilerin izlenmesine yarayan teknik araçlardır." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 165, 166.

"…kişinin gözü ya da kulağıyla nakil halindeki verileri görüntü ya da ses olarak izlemesi halinde bu suç oluşmaz…bilişim sistemine uzaktan bağlantı yapmak suretiyle erişim sağlanması halinde (örneğin teamweaver gibi yazılımlarla) bilişim sistemine girme söz konusu olduğu için bu suç oluşmaz. Dolayısıyla böyle yazılımlarla bilgisayarın ekran görüntüsüne, kamerasına ya da mikrofona ulaşılması ya da casus yazılımlarla mobil bilgisayarın izlenmesi halinde bu suç oluşmaz." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 307, 308.

987 5651 sayılı Kanun' un 2. maddesinin 1. fıkrasının (h) bendinde: "İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini" ifade eder şeklinde tanımlanmıştır. Bkz. https://mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5651&MevzuatIliski=0&sourceXmlSearch=internet%20ortam%C4%B1nda%20yap%C4%B1lan%20yay%C4%B1nlar%C4%B1n%20d%C3%BCzenlenmesi%20ve%20bu%20yay%C4%B1nlar%20yoluyla%20i%C5%9Flenen%20su%C3%A7larla%20m%C3%BCcadele&Tur=1&Tertip=5&No=5651, ET. 19 Mart 2020.

988 Koca ve Üzülmez, a.g.e., s. 823; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 307; Akbulut, *Bilişim Alanında Suçlar*, s. 165.

989 Aynı yönde bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 165, 170.

araçlarla izleme fiili yanında başka bir fiili ile verilerin içeriğini öğrenmesi veya verileri kaydetmesi veya yok etmesi gerçekleşiyor ise fail, gerçek içtima kuralları uyarınca 243/4. m. yanında oluşan ilgili diğer suçlardan da cezalandırılacaktır. Bunun yanında suç, nakledilen verinin izlenmeye başlamasıyla tamamlanmakta olup izleme fiili devam eden bir fiil olduğundan mütemadi (kesintisiz) suç olarak değerlendirilecektir.[990]

3.2.1.9.3. Manevi Unsur

Düzenlenmiş olan suç tipi kasten işlenebilen bir suç olup taksirli hali düzenlenmiş olmadığından taksirle işlenmesi halinde suç teşkil etmeyecektir.[991] Bunun yanında, madde metninde fiilin "hukuka aykırı olarak" işlenmesi özel olarak belirtilmiş olduğundan suç ancak doğrudan kastla işlenebilecek, olası kastla işlenmesi söz konusu olamayacaktır.[992]

3.2.1.9.4. Hukuka Aykırılık

243/4' te düzenlenmiş olan suç tipinde izlemenin hukuka aykırı olması gerektiği ayrıca belirtildiğinden hukuka aykırılık tipikliğe ait bir unsur olarak kabul edilecek ve hukuka özel aykırılık oluşturan bu halde failin gerçekleştirmiş olduğu izleme fiilinin hukuka aykırı olduğunu bilmesi şartı aranacaktır.[993] Suç olarak düzenlenen bu fiile (izlemeye) izin veren bir hukuk kuralının varlığı, yetkili merciin emrini ifa veya verinin ait olduğu kişinin rızası fiili hukuka uygun hale getirecek ve suç oluşmayacaktır.[994] Örneğin, CMK 135, PVSK 13/A, ek 7. m., MİT Kanunu 6. m., Jandarma Teşkilat, Görev ve Yetkileri Kanunu Ek 5. m. uyarınca gerçekleştirilen iletişimin denetlenmesi kapsamında verilerin izlenmesi hukuka uygun kabul edilecek ve bu suçun konusunu oluşturmayacaktır.[995]

Ancak Koca-Üzülmez' e göre, bu suçun gerçekleşebilmesi için fail tarafından veri naklinin engellenmesi, verinin bütünlüğüne müdahale edilmesi ve içeriğinin öğrenilmesi hallerinde haberleşmenin engellenmesi veya haberleşmenin gizliliğini ihlal suçları oluşacağından fail sadece veriyi izlemekle yetinmelidir. Bkz. Koca ve Üzülmez, a.g.e., s. 822.

990 Koca ve Üzülmez, a.g.e., s. 823; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 308.

991 Koca ve Üzülmez, a.g.e., s. 822; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 308; Akbulut, *Bilişim Alanında Suçlar*, s. 168.

992 Aynı yönde bkz. Koca ve Üzülmez, a.g.e., s. 822; Akbulut, *Bilişim Alanında Suçlar*, s. 168.

993 Koca ve Üzülmez, a.g.e., s. 822; Akbulut, *Bilişim Alanında Suçlar*, s. 166.

994 Koca ve Üzülmez, a.g.e., s. 822.

995 Akbulut, *Bilişim Alanında Suçlar*, s. 168.

3.2.2. Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK madde 244/1-2)

TCK' nın 244. m.'si:

"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) 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.

(3) 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.

(4) 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 beşbin güne kadar adlî para cezasına hükmolunur.[996]

şeklinde düzenlenmiştir.

İlgili madde Adalet Komisyonunda[997], birinci ve ikinci fıkrada yer alan eylemler birinci fıkrada yer alacak şekilde düzenlenmiş ve diğer fıkralarda suçun nitelikli halleri kabul edilmiş iken TBMM Genel Kurulu' ndaki görüşmeler esnasında verilen bir önerge ile bilişim sistemlerine yönelik fiiller ile verilere yönelik fiiller arasında ağırlık bakımından farklılık bulunduğu belirtilerek madde düzenlemesinde iki farklı suç kabul edilmiştir.[998]

Maddenin 765 sayılı TCK' da yer alan karşılığı farklılıklar bulunmasına rağmen 525/b m.'si[999] olup maddenin AKSS' de yer alan karşılığı ise 4. ve 5.

---

996 https://mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf, ET. 19 Mart 2020.

997 "Suç tipi, Adalet Komisyonu'nda kabul edilen metinde "Bir bilişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka bir yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir" şeklinde düzenlenmekteydi." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 331.

998 Koca ve Üzülmez, a.g.e., s. 824.

"…Bu değişikliğin gerekçesinde ise; "suç tanımlarında belirliliği sağlamak ve ceza miktarlarını işlenen fiilin ağırlığına uygun olarak belirlemek amacıyla madde metninde değişiklik yapılması uygun görülmüştür" denilmiştir. Bu noktada belirtmeliyiz ki TCK'nın 244'üncü maddesinin gerekçesi düzenlenirken TBMM genel kurulundaki değişikliğe yer verilmeyerek ilk iki fıkranın gerekçesi ortak bir şekilde kalmıştır." Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 180.

999 "Başkasına zarar vermek veya kendisine veya başkasına zarar yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beşmilyon liradan ellimilyon liraya kadar ağır para cezası verilir." Bkz. Özbek, v.d., a.g.e., s. 930.

"- 765 sayılı TCK'da bu suçun olmazsa olmaz şartı olarak başkasına zarar vermek veya kendisine ve başkasına yarar sağlamak maksadıyla yapılması hususunun öngörülmesine karşın, YTCK'nın 244/3. maddesiyle kendisi veya başkasına yarar sağlama nitelikli hal sayılmış, ayrıca failde zarar verme amacının bulunması aranmamıştır.

m.'leridir. Buna göre, AKSS'nin 4. m.' sinde yer alan düzenlemede verinin konumu ya da nerede saklandığı konusunda farklılık yaratılmamış, 5. m.'de ise sisteme veri yoluyla müdahale edilmesi veya sistem içerisindeki verilere müdahale edilmesi esas alınarak sistemin işleyişine fiziki müdahaleler madde kapsamında değerlendirilmemiştir.[1000]

TCK'nın 244. m.'sinin birinci fıkrasında, bilişim sisteminin işleyişini engelleme veya bozma suçu ikinci fıkrasında bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma suçu düzenlenmiş olup 3. fıkrada 1. ve 2. fıkrada yer alan fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali nitelikli hali ve 4. fıkrada ise bu fiillerin işlenmesi suretiyle haksız yarar sağlanması suçu düzenlenmiştir. Her ne kadar 4. fıkra düzenlemesinin ayrı bir suç mu yoksa nitelikli hal mi olduğu konusunda doktrinde fikir birliği bulunmasa da biz ilgili başlık altında açıklanacağı üzere 4. fıkra düzenlemesini de ayrı bir suç düzenlemesi olarak kabul ediyor ve ayrı bir başlık altında unsurları ile birlikte incelemeyi uygun görüyoruz. Bu bağlamda, 1. ve 2. fıkrada yer alan suçların unsurları ortak başlıklar altında farklılaştıkları noktalara ayrıca değinilerek incelenecek olup her iki suç bakımından ortak nitelikli hal olarak kabul ettiğimiz 3. Fıkra düzenlemesi suçun nitelikli halleri ve 4. fıkrayı ise ayrı bir suç başlığı unsurları ile birlikte ayrıca incelenecektir.

3.2.2.1. Korunan Hukuksal Değer

TCK'nın 244. m.'sinin 1. ve 2. fıkralarında düzenlenen suç tipleri açısından korunan hukuksal değer bakımından doktrinde farklı görüşler bulunmaktadır. Yaşar, Gökcan, Artuç' a göre TCK 244. m.'nin gerekçesinde mala zarar verme suçunun özel bir şekli düzenlendiği belirtildiğinden bu suç ile korunan ilk hukuksal yarar malvarlığı değerleri olup bu suç ile toplumun önemli bir kesimi tarafından kullanılan bilişim

-765 sayılı TCK'da suçun konusu olarak "bilgileri otomatik işleme tabi tutmuş bir sistem veya veriler veya diğer herhangi bir unsurdan", bahsedilmesine karşın, YTCK ile suçun konusu olarak bilişim sistemi ve verilerden söz edilmektedir.
-765 sayılı TCK'da suçun hareket unsuru olarak "tahrip etmek, değiştirmek, sistemin işleyişine engel olmak, sistemin yanlış biçimde işlemesini sağlamak" olarak gösterilmişken; YTCK'da suçun hareket unsuru olarak "sistemin işleyişini engellemek, bozmak, verileri bozmak, yok etmek, değiştirmek, erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka yere göndermek" belirlenmiştir.
-765 sayılı Kanunun 525/c maddelerinde yer alan " hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturma" ibaresine yer verilmemiş ancak genel olarak " hukuka aykırı veri yerleştirme veya değiştirme" seçimlik hareketleri metne dahil edilmiştir." Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7306.
1000 Özbek, v.d., a.g.e., s. 930.

sistemine veya bu sistemin içerdiği verilere zarar verildiğinde bilişim sistemi kullanan kişilerin güveni sarsılabileceğinden aynı zamanda bilişim sistemine olan güven de korunmaya çalışılmaktadır.[1001] Yılmaz' a göre de bu suçun konusu mala zarar verme suçunun hukuki konusuyla örtüşmekte olup yapılan düzenleme ile bilişim sistemi veya veriler üzerinde sahibi veya zilyedinin her türlü mülkiyet hakkı ve buna bağlı olarak toplum menfaati korunmak istenmektedir.[1002] Karagülmez de, 244. m.'nin gerekçesinde belirtildiği üzere sistemlere yönelik ızrar fiillerinin özel bir suç haline getirme düşüncesi olduğundan ve suçun konusunu bilişim sisteminin varlığı ve işlemesini sağlayan bütün unsurlar oluşturduğundan 1. ve 2. fıkralarda korunan hukuksal değerin, hem bilişim sisteminin hem de sistem içerisinde yer alan veriler ya da diğer unsurların zarar görmemesi olduğunu belirtmektedir.[1003] Diğer bir görüşe göre, Erdoğan' ın da belirttiği gibi, her saldırı kişilerin sisteme olan güvenini etkileyeceğinden ve maddenin düzenlendiği bölümün topluma karşı olduğu dikkate alındığında korunan hukuksal değer öncelikle sistemin toplum açısından güvenilirliği ve toplumun tamamının menfaatleri olup sistem sahibinin ve kullanıcısının maddi ve

1001 Yaşar, Gökcan, Artuç' a göre, verinin ele geçirilmesi suçu Alman Ceza Kanunu'nda malvarlığına karşı suçlar arasında mala zarar verme suçundan sonra düzenlenmiş hatta 765 sayılı TCK'da da bilişim alanında suçlar malvarlığına karşı suçlar bölümünden hemen sonra koyularak malvarlığının korunmasına işaret etmektedir. Ancak klasik malvarlığına karşı işlenen suçlarda malvarlığına verilen zarar sonrasında sadece malvarlığı sahibi etkilenirken bu suç ile bilişim sistemi ile irtibatlı olan herkesin bilişim sistemine olan güveni de korunmaya çalışılmaktadır. Zira, bu suç "kişilere karşı suçlar" kısmının "malvarlığına karşı suçlar" bölümünde düzenlenmemiş, "topluma karşı suçlar" kısmında düzenlenmiş, sistemin ve içeriğinin uygun şekilde işlev görmesiyle başta malikin veya sistemi kullanan kimselerin yararın da korunduğu belirtilmektedir. Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7307.

1002 Yılmaz' a göre, "Bilindiği üzere mala zarar verme suçunda korunan hukuki değer, iktisaptan farklı olarak, kullanılırlık veya yararlılık değerini azaltan, yok eden fiillere karşı, mülkiyeti korumaya ilişkin toplumsal menfaattir.

…Kanun sistematiği bakımından, suçla korunan hukuki değerin mala zarar verme suçu ile aynı amaca hizmet ettiği gözetildiğinde, şu husus önemli bir eksiklik olarak ortaya çıkmaktadır. Şöyle ki, mala zarar verme suçu Ceza Kanunu'nun İkinci Kısım Onuncu Bölüm'ünde yer alırken; TCK'nın 244 maddesi Üçüncü Kısım Onuncu Bölüm'de yer almaktadır. Mala zarar verme suçunu işleyenler, aynı bölüm içerisinde yer alan TCK 167 maddesinde yazılı şahsi cezasızlık sebepleri ile TCK'nın 168 maddesinde yazılı etkin pişmanlık hükümlerinden yararlanma olanağına sahiptir.

Mala zarar verme suçu ile aynı hukuki değeri koruyan TCK'nın 244. maddesi, kanun sistematiğinde İkinci Kısım Onuncu Bölüm'de yer alsa idi, TCK'nın 244. maddesinde yazılı suçu işleyenler yukarıda yazılı yasal olanaklardan yararlanabilecekti. Benzer bir eleştiri TCK'nın 245. maddesi için de geçerli idi. Ancak 5377 sayılı Kanun'un 27. maddesi ve 5360 sayılı Kanun'un 11. maddesi ile bu eksiklikler giderilerek, TCK'nın 245. maddesi için faile etkin pişmanlık ve şahsi cezasızlık sebeplerinden yararlanma olanağı getirilmiştir. Kanaatimizce benzer bir düzenlemenin TCK'nın 244. maddesi için de yürürlüğe konması gereklidir." Bkz. Sacit Yılmaz, "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", *Türkiye Barolar Birliği Dergisi,* Sayı: 92, Yıl: 23, Ocak-Şubat 2011, ss. 62-100, s. 68, 69.

Eker' e göre de madde gerekçesinde bilişim sistemlerine yönelik ızrar fiilleri ayrıca düzenlenerek özel bir suç sayılmış, bu norm ile bilişim sistemine ilişkin mülkiyet hakkı korunmuştur. Bkz. Eker, a.g.e., s. 124.

1003 Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,* s. 215.

manevi çıkarlarının yanında bilişim sisteminin güvenliği de korunmak istenen diğer menfaatlerdir.[1004] Koca-Üzülmez' e göre de, 244. m.'nin ilk iki fıkrasında düzenlenen suçlar ile korunan hukuksal değer, her ne kadar bu fiiller bireyin malvarlığı değerini ihlal etse de Kanun'un sisteminde düzenlendiği yer göz önünde bulundurulduğunda bireyin malvarlığına dahil bir değer olmasından ziyade bilişim sistemlerinin doğru bir şekilde işleyişini korumaktır.[1005] Özbek ve diğerlerine göre bu madde ile korunan değer temel olarak iki tane olup birincisi, bir bütün olarak bilişim sisteminin ve verilerin güvenliği, ikinci olarak korunan değer ise mülkiyet hakkıdır.[1006] Akbulut' a göre, 1. fıkrada yer alan "sistemin işleyişinin engellenmesi veya bozulması" ifadeleriyle herhangi bir problem olmadan tüm bilişim sistemleri sahiplerinin, işletmecileri ile kullanıcılarının sistemin arızasız çalışmasındaki yararı, ikinci fıkrada ise veriler üzerinde tasarruf yetkisi olan kişilerin verilerin bozulmadan veya müdahale olmadan kullanılmasındaki yararı korunmaktadır.[1007] Mahmutoğlu' na göre ise korunan hukuksal değer, bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisine sahip kişinin, verilerle oluşturulan değerlerine herhangi bir engel veya gecikme olmadan ulaşması ve kullanmasıdır.[1008] Dülger' e göre de, bu suçlarla korunan hukuksal değer bilişim sistemi veya bilişim sistemi içinde yer alan veriler üzerinde tasarruf yetkisi bulunan kişinin, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. değerlerine gecikme olmadan ulaşması ve kullanmasındaki

1004 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 184.
Erdoğan, 244. maddenin 2. fıkrasında düzenlenen suç açısından ise birden çok korunan değer olup bunlar verilerin gizliliği ve dokunulmazlığı, mülkiyet hakkı, malvarlığı hakkı, verinin içeriğine göre fikri mülkiyet hakkı ve tüm bilişim suçlarında olduğu gibi bilişim sisteminin güvenilirliğidir. Ayrıntılı bilgi için Bkz. A.e., 214-216.
1005 Koca ve Üzülmez' e göre, bilişim sistemlerinin günümüzde artık toplumsal yaşamın vazgeçilmez araçları haline gelmesi sebebiyle bu sistemlerin hukuk tarafından bireyin malvarlığına dahil bir unsur olmasının ötesinde korunmasını gerekli kılmaktadır. Örneğin, ÖSYM gibi devlet kurumlarının sistemlerine yapılan saldırılar milyonlarca insanın mağduriyetine yol açabilmektedir. Bkz. Koca ve Üzülmez, a.g.e., s. 825.
1006 "…Çünkü gerek birinci gerekse ikinci fıkrada düzenlenen eylemlerle hem bilişim sisteminin işleyişi hem de veriler hedef alınmıştır. Fakat burada bir hususun altı çizilmelidir. TCK m. 244/2'deki eylemlerin hedefi konumundaki veriler, bir bilişim sisteminin unsuru niteliğinde olmayan ve fakat bir bilişim sistemi içinde tek başlarına bulunan unsurlardır. Çünkü söz konusu veriler bir bilişim sisteminin işleyişi bakımından unsur niteliğindeyse, o halde bu veriler artık bilişim sistemi içinde değerlendirilir.
İkinci olarak korunan hukuki değer ise mülkiyet hakkıdır. Zira TCK m. 244/1 ve 2'de düzenlenen eylemler, sahibinin söz konusu bilişim sistemi ve veri üzerinde tasarrufta bulunma yetkisine açık bir tecavüz niteliği taşımaktadır. Yine aynı şekilde TCK m. 244/4'te de, anılan bu eylemleri gerçekleştirilmek suretiyle haksız menfaat temin etme düzenlendiği için, TCK m. 244'ün aynı zamanda bir bütün olarak mülkiyet hakkını da koruduğunu söylemek mümkündür." Bkz. Özbek, v.d., a.g.e., s. 932.
1007 Akbulut, *Bilişim Alanında Suçlar*, s. 181.
1008 Mahmutoğlu, a.g.e., s. 866.

çıkar başka bir deyişle, bilişim sisteminin ve bu sistem içerisinde yer alan verilerin veya diğer unsurların sağlam ve güvenli bir şekilde çalışılabilirliğinin korunmasıdır.[1009] Artuk- Gökçen- Yenidünya' ya göre de, bu suç ile bilişim sistemlerinin işletmeci ve kullanıcılarının, bu sistemleri uygun biçimde işletme hakları korunmakla birlikte suç tipinin ihdasıyla bilişim sistemlerinin doğru ve işlevine uygun şekilde faaliyetlerine devamları sağlanmak istenmektedir.[1010] Soyaslan' a göre suç birden fazla hukuki değeri korumakta olup bilişim sistemlerinin veri ve yazılımlarından oluşan soyut unsurları ile donanım kısmını oluşturan somut unsurları bunun yanında, bilişim sistemi ve içerdiği veriler, üzerinde tasarruf yetkisi bulunan kişinin, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma gibi değerlere herhangi bir engel, arıza veya gecikme olmadan ulaşılması ve kullanılmasındaki yararı korumaktadır.[1011] Kurt' a göre, bu suç ile öncelikle mülkiyet hakkı korunma altına alınmakta olup 1. fıkrada, bilişim sistemi sahibinin mülkiyet hakkı, zilyedin ise bilişim sisteminin dokunulmazlığı, iletişim kurma ve teknolojik gelişim özgürlüğü, 2. fıkrada ise mülkiyet hakkı, verilerin içeriğine göre ise fikri mülkiyet hakkı, özel hayatın gizliliği ve ticari sırlar korunmaktadır.[1012] Son olarak Apaydın' a göre ise bilişim sistemini bozma veya engelleme suçlarında korunan hukuksal değer dar anlamda bireylere ait bilişim sistemlerinin işleyişi ve güvenliği ile iletişim ve mülkiyet haklarının korunması, geniş anlamda ise ülke ekonomisi, kamu güvenliği ve kamu düzeninin korunmasıdır.[1013]

1009 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 313, 314.

1010 Artuk, Gökcen ve Yenidünya'ya göre, AKSS' nin açıklayıcı raporunda da belirtildiği üzere, bu suç tipi "bilgisayar sabotajı" olarak nitelendirilen fiilleri önlemeyi amaçlamakta olup bilişim sisteminin engellenmesi veya bozulması, sistemin hem donanımına hem de yazılımına zarar verici niteliktedir. Bunun yanında, internetin günümüz hayatında geldiği nokta göz önünde bulundurulduğunda, bilişim sisteminin işleyişinin engellenmesi ve bozulması haberleşme özgürlüğünü de sınırlayan ve ortadan kaldıran bir nitelik arz etmektedir. Yine, 2. fıkrada düzenlenen suç açısından ise, bilgisayar verilerini ve bilgisayar programlarını, fiziksel nesneler gibi kasıtlı zarar verme girişimlerinden korumaktır. Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6927, 6932.

1011 Soyaslan, a.g.e., s. 641, 642.

1012 "Bu hükümle hem fizik, hem de soyut kavramlar koruma altına alınmaktadır. Kanun koyucu bu fiillerin meydana getirdiği sosyal zararların büyüklüğünü de dikkate almak suretiyle suç haline getirmektedir. Sistemin ve sistem içinde yer alan verilerin dokunulmazlığı korunan hukuki yarardır." Bkz. Kurt, a.g.e., s. 161, 162.

Aynı yönde bkz. Parlar ve Hatipoğlu, a.g.e., s. 3746, 3749.

Gül' e göre de, günümüzde bilişim sistemlerinin kurulması, işleyişi, içerdiği veriler önemli bir ekonomik maliyet oluşturduğundan bunlara zarar verme halinde de önemli ekonomik zararlar oluşmaktadır. Bu doğrultuda ilk iki fıkrada korunan hukuksal değer mülkiyet hakkı olup ayrıca verilerin başka yere gönderilmesi halinde üçüncü kişilerin özel hayatına ve haberleşme hürriyetine de müdahale söz konusu olmaktadır. Bkz. Gül, a.g.e., s. 86.

1013 Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 213, 230.

244. m.'nin 1. fıkrasının AKKS' de karşılığı olan "Sistem Engellemeleri" başlıklı 5. m.'nin dayanak raporunda, korunan hukuksal yararın bilgisayar verilerine veya programlarına zarar verilmesi, veri ve programların bozulması veya zarar görmesini engellemek ve böylece doğru ve işlevsel olarak çalışmalarını sağlamak, 244. m.'nin 2. fıkrasının karşılığı olan "Veriye Müdahale" başlıklı 4. m.'sinin dayanak raporunda ise bilişim sistemi kullanıcılarının ve operatörlerinin fonksiyonlarına uygun şekilde bu sistemi kullanma hakları olduğu belirtilmiştir.[1014]

Kanaatimizce, 244. m.'nin 1. ve 2. fıkralarında düzenlenen suç tipleri ile korunmak istenen hukuksal değer, karma nitelikte olup dar anlamda bilişim sisteminin ve verilerin güvenliği[1015] ve bilişim sistemleri ve veriler üzerinde tasarruf yetkisi bulunan kişilerin, bu sistemi ve bu sistem içerisindeki verilerini herhangi bir engel olmadan kullanmasındaki yararı, geniş anlamda ise Erdoğan' ın da belirttiği gibi, sistemin toplum açısından güvenilirliği başka bir deyişle bilişim sisteminin güvenilirliği ve toplumun tamamının menfaatleri korunmak istenmektedir. Her ne kadar madde gerekçesinde bu madde ile düzenlenen suç tipinin mala zarar vermenin özel bir hali olduğu belirtilmişse de birbirine ağlarla bağlı birçok bilişim sisteminin ve bu sistemlerin sunmuş olduğu hizmetlerin var olduğu günümüzde bir bilişim sistemine gerçekleştirilecek bir saldırının diğerine açık bir tehdit oluşturduğu gerçeği karşısında tüm bilişim alanında suçlarda olduğu gibi ve Apaydın'ın da belirtmiş olduğu gibi kamu güvenliği' nden kamu düzenine kadar ve aslında bu alanın tamamına yönelik bir koruma sağlanmak istendiği söylenebilecektir. Nitekim, Erdoğan' ın da belirtmiş olduğu gibi maddenin düzenlendiği bölümün topluma karşı olduğu dikkate alındığında ve maddenin 3. fıkrasında, 1. ve 2. fıkralarda yer alan fiillerin bir banka veya kredi kurumuna ya da bir kamu kurumuna ait bilişim sistemi üzerinde işlenmesi halinin cezayı artırıcı nitelikli bir hal kabul edilmesi ile bu "sistemlerin düzgün çalışmaması halinde toplumun tamamının mağdur olacağı"[1016] esasından hareketle toplumun tamamının korunmak istendiğinin başka bir göstergesini oluşturduğu düşünülmektedir.

1014 Parlar ve Hatipoğlu, a.g.e, s. 3749.
1015 Bundan kasıt sistemin kesintisiz ve sağlıklı çalışmasıdır.
1016 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 198.

3.2.2.2. Maddi Unsur

3.2.2.2.1. Fail ve Mağdur

TCK m. 244' ün 1. ve 2. fıkralarında düzenlenen suç tiplerinde fail ve mağdur için herhangi bir özellik aranmadığı gibi sınırlama da getirilmemiştir.[1017] O halde bu maddede düzenlenen suç tipleri açısından herkes fail ya da mağdur olabilecektir. Bu bağlamda, bilişim sisteminin işleyişini engelleyen, bozan, bilişim sistemindeki verileri bozan, yok eden, değiştiren, erişilmez kılan, sisteme veri yerleştiren veya var olan verileri başka yere gönderen kişi bu suçun faili olabilecektir.[1018] Ancak suç, bir tüzel kişinin faaliyeti çerçevesinde tüzel kişiliğin organ veya temsilci sıfatını taşıyan gerçek kişiler tarafından gerçekleşirse bu durumda tüzel kişi hakkında bunlara özgü güvenlik tedbirlerine hükmolacaktır.[1019]

Mağdur açısından bakıldığında ise, doktrinde bilişim sistemi veya veriler üzerinde hak sahibi olan gerçek veya tüzel kişinin mağdur olabileceği belirtilmekte olup mağdur, bilişim sisteminin maliki veya zilyedi olabileceği gibi bilişim sistemi üzerinde "tasarruf yetkisi olan"[1020] bir kişi de mağdur olarak kabul edilebilecektir.[1021]

1017 Yaşar, Gökcan ve Artuç, a.g.e., s. 7307; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6929.

1018 Yaşar, Gökcan ve Artuç, a.g.e., s. 7307.

Soyaslan' a göre failin belirlenmesi açısından, "Eğer fiil bilişim sistemine yönelik olarak gerçekleştirilmişse sistemin kendisinin, bilişim sisteminin içerdiği verilere yönelik gerçekleştirilmişse bu verilerin, hem bilişim sistemine hem de verilere karşı gerçekleştirilmişse her ikisinin de ayrı ayrı mülkiyet, kullanım ve tasarruf haklarının kime ait olduğunu ve zararı kimin meydana getirdiğini açıkça ortaya koymak gerekir." Bkz. Soyaslan, a.g.e., s. 642. Aynı yönde bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 316.

1019 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6929.

1020 "Tasarruf yetkisi noktasında malik benzeri (eigentümerähnlicher9 veri tasarruf yetkisi belirlemesi yapılmaktadır. Malik benzeri hak olarak veri tasarruf yetkisi karakteri, asıl veri tasarruf yetkisinin eşya hukukuyla ilişkili bilişim sistemiyle (veri taşıyıcısıyla) bağlantılı olarak belirlenmesini desteklemektedir. Bu nedenle tasarruf yetkisi bilişim sisteminin sahibine veya hukuka uygun zilyedine aittir." Ayrıntılı bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 187.

1021 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, s. 195; Parlar ve Hatipoğlu, a.g.e., s. 3750.

"…Bu itibarla suçun oluşmasına yol açan eylemler nedeniyle, bilişim sistemindeki verilere geç ulaşan, hiç ulaşamayan, sistemi kullanamayan ve sistem üzerinde tasarruf yetkisi bulunan kimse, çıkarları zedelendiği için suçun mağduru olacaktır. Bu noktada mağdur bilişim sistemi üzerinde mülkiyet hakkına sahip olan ya da sistem üzerinde zilyetlik hakkı bulunan herhangi bir kimse olabilmektedir. Bu suçları oluşturan hareketlerin gerçekleştirilmesi sonucunda; bilişim sistemine ve/veya verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşılmasında ve kullanılmasında çıkarı bulunan ve bilişim sistemi ve/veya veriler üzerinde tasarruf yetkisi bulunan kişi bu suçun mağduru olacaktır." Bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 215; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 317.

Artuk-Gökçen-Yenidünya' ya göre bilişim sistemi ile verilerin sahibi farklı kişiler olabileceğinden her ikisinin de suçun mağduru olduğunu kabul etmek gerekir. Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6935.

Bunun yanında, 3. fıkrada düzenlenen nitelikli hal bakımından ise banka veya kredi kurumu veya kamu kurum veya kuruluşunun mağdur ya da suçtan zarar gören olarak mı değerlendirileceği hususunda doktrinde suçun mağduru olarak kabul edileceği görüşünün hakim olduğu belirtilmekte[1022] ise de kanaatimizce tüzel kişiler mağdur sıfatına haiz olamayacağından suçtan zarar gören olarak kabul edilmelidir.

3.2.2.2.2. Suçun Konusu

244. m.'nin 1. ve 2. fıkralarında düzenlenmiş olan suçların konuları birbirinden farklı olup doktrinde tartışmalı olsa da kanaatimizce 1. fıkrada yer alan suçun konusu "bilişim sisteminin işleyişi"[1023] iken 2. fıkrada yer alan suçun konusu ise bilişim sisteminin içerdiği verilerdir.[1024] Madde gerekçesi:

> *"Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır."*[1025] şeklinde düzenlenmiş olduğundan doktrinde suçun konusuna ilişkin görüşlerde bir takım farklılıklar oluşmuştur.

Dülger' e göre de bilişim sistemine, verilere veya veri işleme zarar veren kişinin bilişim sisteminin maliki veya kullanım hakkı sahibi olmasına göre suçun mağduru da değişecektir. Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 317.

1022 Özbek, v.d., a.g.e., s. 935.

Soyaslan' a göre bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunda her gerçek veya tüzel kişi suçun mağduru olabilecektir. Bkz. Soyaslan, a.g.e., s. 642.

Ancak Apaydın' a göre tüzel kişiler ancak suçtan zarar gören olabilmektedir. Bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 215.

Yine Akbulut' a göre de mağdur ancak gerçek kişi olabileceğinden tüzel kişiler suçtan zarar gören olabilir. Dolayısıyla kamu kurum ve kuruluşlarının bilişim sistemlerine karşı bu suçun işlenmesi halinde toplumu oluşturan herkes suçun mağduru olacaktır. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 185.

1023 Aynı yönde bkz. Koca ve Üzülmez, a.g.e., s. 826.

Yaşar, Gökcan, Artuç'a göre ise, 244. maddenin 1. fıkrasında düzenlenen suçun konusu "bilişim sistemi" dir. Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7308.

1024 Aynı yönde bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6935; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 316; Yaşar, Gökcan ve Artuç, a.g.e., s. 7311.

Erdoğan' a göre: "…ikinci fıkrada korunan veriler bilişim sisteminin işleyişine ilişkin veriler olmayıp sistemin içerisinde bulunan, ancak sistemin işleyişine etkisi olmayan verilerdir. Zira bilişim sisteminin işleyişini etkileyecek verilere müdahale halinde birinci fıkranın tatbiki gerekecektir. Diğer bir deyişle, ikinci fıkrada sistemin içinde yer alan ancak sistemin yapıtaşı olmayan veriler korunmaktadır." Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 215.

1025 Gül, a.g.e., s. 85.

Erdoğan' a göre, bilişim sisteminin engellenmesi ve bozulması suçunun konusu bilişim sisteminin fiziki varlığı ve işlemesini sağlayan tüm unsurlar yer almakta başka bir deyişle bu suç ile bilişim sisteminin tüm unsurları korunmakta olup içinde veri bulunmasa dahi bilişim sisteminin temel özellikleri olan veri alma, depolama ve gönderme özelliklerine sahip bilişim sistemleri korunmalıdır.[1026] Özbek ve diğerlerine göre ise, bir bilişim sisteminin işleyişi bakımından unsur niteliği taşımak koşulu ile gerek yazılım gerekse donanım unsurları suçun konusunu oluşturmaktadır.[1027] Artuk-Gökçen-Yenidünya' ya göre de TCK' nın 244. m.'sinin gerekçesi de dikkate alındığında bilişim sisteminin işleyişinin engellenmesi veya bozulması, sistemin hem donanımına hem de yazılımına zarar verici niteliktedir.[1028] Apaydın'a göre ise, suçun konusu içinde veriler bulunan bir bilişim sisteminin yazılımıdır zira diğer herhangi bir eşyadan öteye gidemeyen bir bilişim sisteminin donanımına yönelik eylemler failin kastına göre TCK' nın 151. m.'sinde yer alan mala zarar verme suçunu oluşturacaktır.[1029] Soyaslan' a göre de içinde hiçbir veri bulunmayan bir bilişim sistemi bu suçun konusunu oluşturmayacak böyle bir sisteme yönelik eylemlerde ve failin kastı sadece mala zarar verme olduğunda TCK' nın 151. m.'si uygulanacaktır.[1030]

1026 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, s. 195, 196.

1027 "…bilişim sistemi yazılımı ve donanımıyla bir bütündür. Yazılım olmadan donanım, donanım olmadan da yazılım tek başına bir anlam ifade etmez. Tersinden hareket edilecek olursa yazılıma verilecek bir zarar hiç şüphe yok ki donanımın da işlevselliğine olumsuz yönde etkide bulunacaktır. Bir örnekle açıklamak gerekirse; yüksek kapasiteli ve yüksek hızlı, bilgisayara monte edilmiş, teknik müdahale haricinde çıkarılamayan, manyetik usullere göre bilgi okuyup yazan hard disk bir donanım unsurudur. Ancak hard disk tek başına maddi varlığı ile bu işlemleri gerçekleştiremez. Bu işlevleri gerçekleştirebilmesi için hard diske BIOS adı verilen yazılımın (programın) yüklü olması gerekmektedir. Bu anlamda bir bilgi işlem faaliyeti için yazılım – donanım uyumluluğunun zorunluluğu görülmektedir. Dolayısıyla TCK m. 244/1 anlamında bilişim sisteminin işleyişinin bir unsuru olmak koşulu ile gerek yazılım gerekse donanım unsurları suçun hukuki konusu dâhilinde düşünülebilir." Bkz. Özbek, v.d., a.g.e., s. 933, 944.

1028 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6927.

1029 Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 215.

Aynı yönde Yaşar, Gökcan ve Artuç' a göre de; "…her ne kadar bu suçla ilgili korunan hukuki yararlardan birisi malvarlığı değeri ise de, YTCK'nın 244. maddesinde düzenlenen suçun konusunu, bilişim sisteminin veya daha dar bir deyişle bilgisayarın fiziksel, donanımla ilgili bölümü değil, soyut olan programlara ve yazılıma ilişkin yanıdır…bir kimsenin bilgisayarının kırılması veya internet bağlantısını oluşturan kablonun kesilmesi eylemi kanaatimizce bu suçu değil, genel mala zarar verme suçunu (YTCK'nın 151. md) oluşturacak, bilgisayar ve diğer bilişim sistemlerinin içinde yer alan yazılımlara zarar verilmesi halinde, bu madde hükümleri uygulanacaktır..." bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7308.

1030 "…Çünkü; maddenin düzenlenme amacı bilişim sisteminin somut yapısı olan donanım unsuruna verilen zararları cezalandırmak değil, bilişim sisteminin soyut unsurları olan verilerde ve bilişim sisteminin işleyişinde meydana getirilen zararları cezalandırmaktır." Bkz. Soyaslan, a.g.e., s. 643.

Aynı yönde bkz: "…bu maddenin düzenlenme amacı klasik anlamda bilişim sisteminin somut yapısı olan donanım unsuruna verilen zararları cezalandırmak değil, bilişim sisteminin soyut unsurları olan

Kanaatimizce, ilgili başlıkta da belirtmiş olduğumuz üzere bir bilişim sistemi donanım ve yazılım hatta ağ unsurları ile bir bütün oluşturduğundan 244. m.'nin 1. fıkrasında yer alan suçun konusu için bütünü itibariyle bilişim sisteminin işleyişi olduğunu söyleyebiliriz. Zira 244. m.'nin 1. fıkrasında korunan hukuksal değerin olarak da dar anlamda bilişim sisteminin güvenliği olduğunu belirtmiştik. Bu doğrultuda failin kastı bir bilişim sisteminin işleyişine yönelik olduğu sürece fiilin bilişim sisteminin donanım ya da yazılım unsuruna karşı gerçekleştirilmiş olması fark yaratmamalıdır. Zira, fail donanım unsuruna gerçekleştirileceği bir fiille de bilişim sisteminin işleyişine engel olabiliyorsa burada failin kastı dikkate alınarak 244. m.'nin 1. fıkrası uyarınca cezalandırılabilecektir. Kaldı ki bir fiil ile birden fazla farklı suçun oluşması mümkün ve bu halde fikri içtima hükümlerince faile en ağır ceza uygulanacağından böyle bir halin varlığı halinde fail yine 244. m.'nin 1. fıkrası uyarınca cezalandırılacaktır. Ancak failin kastı bilişim sistemini engelleme veya bozmadan ziyade salt bir eşya olarak mala zarar vermeye yönelik ise bu durumda TCK' nın 151. m.'sinde yer alan mala zarar verme suçunun oluştuğu kabul edilebilecek ve bu suçtan cezalandırılacaktır. Yine içinde veri bulunmayan bilişim sistemlerinin bu suçun konusunu oluşturup oluşturmayacağı hususunda doktrinde yer alan maddenin düzenleniş amacı bilişim sisteminin somut yapısı olan donanım unsurlarına verilen zararları cezalandırmak olmadığından içinde veri bulunmayan bir bilişim sistemi ya da veri taşıma aracı bu suçun konusunu oluşturmayacağı yönündeki fikre[1031] katılmaktayız zira bir bilişim sistemi donanım, veri ve ağ unsurlarından oluştuğundan içinde veri bulunmadığından bir bilişim sistemi olarak kabul edilmeyerek bu suçun konusunu da oluşturamayacaktır.

---

verilerde ve bilişim sisteminin işleyişinde meydana getirilen zararları cezalandırmaktır. Her ne kadar 244. maddenin gerekçesinde "böylece sistemlere yöneltilen ızrar fiilleri özel bir suç haline getirilmiştir, aracın fizik varlığı ve işlenmesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır" denilmekteyse de bana göre, bu hatalı bir açıklamadır. Maddenin metninden bu sonuç çıkmamaktadır; gerekçeler de yalnızca maddelerin daha iyi açıklanmasını ve yasa koyucunun görüşünü yansıtması için konulmaktadır; ancak yargılama makamları açısından bağlayıcı değildir. Bu yasa metninin, gerekçede olduğu gibi anlaşılması ise hem TCK'da yer alan 151. ve 244. maddeler arasında uyumsuzluk yaratır hem de inceleme konusu suçun, suç politikası açısından yerinde olmayan bir şekilde uygulanmasına yol açar. Çünkü bilişim sisteminin içinde veri bulunmadığı ya da failin kastının bilişim sisteminin işleyişine ya da içerdiği verilere zarar vermek olmadığı, failin "yalnızca mala zarar vermek" kastıyla hareket ettiği durumlarda 151. maddenin uygulanmayıp 244. maddenin uygulanması hatalı olur." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 317, 318.

1031 Bkz. Soyaslan, a.g.e., s. 643. Aynı yönde bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 195, 196; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 317, 318; Gül, a.g.e., s. 68.

TCK' nın 244. m.'sinin 2. fıkrasında yer alan suçun konusunu oluşturan veri kavramı ile ilgili olarak ilgili başlık altında ayrıntılı açıklamalara yer vermiş olduğumuzdan burada ek bir açıklama yapılmayacaktır.

3.2.2.2.3. Fiil

TCK'nın 244. m.'sinin 1. ve 2. fıkralarında farklı fiiller yaptırım altına alındığından bu suç tiplerini oluşturan eylemler iki başlık altında incelenecektir.

3.2.2.2.3.1. Bilişim Sisteminin İşleyişini Engellemek veya Bozmak

TCK'nın 244. m.'sinin 1. fıkrasında bilişim sisteminin işleyişinin engellenmesi veya bozulması cezai yaptırım altına alınmış olduğundan 1. fıkrada düzenlenen suç tipi neticeli bir suç olarak kabul edilecektir.[1032] Zira bilişim sisteminin işleyişinin engellenmesi veya bozulması hareketin bir sonucudur. Doktrinde bu suçun seçimlik hareketli olduğu belirten yazarlar[1033] bulunmakta olup kanaatimizce de engelleme veya bozulmayı gerçekleştirebilecek nitelikte bir hareket ile[1034] bu suç gerçekleştirilebileceğinden başka bir deyişle madde metninde düzenleme altına alınan suçun oluşumu için gereken netice olduğundan bu suç için serbest hareketli ve hareketlerden herhangi birinin gerçekleştirilmesi ile suç oluşabileceğinden seçimlik hareketli suçtur.[1035] Zira suçu oluşturabilecek neticeler suç tipinde düzenlenmiş ancak

1032 Aynı yönde bkz. Akbulut, Bilişim Alanında Suçlar, s. 190; Koca, Üzülmez, a.g.e., s. 827.
Soyaslan' a göre de: "Suçun neticesi bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi, veya değiştirilmesidir. Söz konusu neticeler zararı oluştururlar. Netice hareket yapıldığı anda gerçekleşir. Neticesi harekete bitişik suç söz konusudur.
…Hareketlerin yapılmasından sonra engellenme, bozulma ve yok edilme veya değiştirilme ile suç tamamlanacaktır." Bkz. Soyaslan, a.g.e., s. 643.

1033 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6928; Yaşar, Gökcan, Artuç, a.g.e., s. 7310, 7320; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 216; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 319, 320; Eker, a.g.e., s. 124, 125; Kurt, a.g.e., s. 164; Parlar ve Hatipoğlu, a.g.e., s. 3749.
Özbek, v.d.' ne göre ise, bilişim sisteminin engellenmesi veya bozulması seçimlik hareketler olarak düzenlenmiş olup bu iki hareketten sadece birinin gerçekleşmesi yeterli olduğundan bağlı hareketlidir. Ayrıca bu suç tipinde ayrıca bir neticenin gerçekleşmesine ilişkin açıklık bulunmadığından sırf hareket suçudur. Bkz. Özbek v.d., a.e.g., s. 937, 938.

1034 Nitekim, bu suç Artuk vd.' nin belirtmiş olduğu gibi bilişim sistemi kullanılmadan örneğin bir iç ağda bilgisayarları birbirine bağlayan kabloların kesilmesi suretiyle de gerçekleştirilebilecektir. Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6928.

1035 Erdoğan, bilişim sisteminin engellenmesinin, sisteme bilişim verilerinin girilmesi, nakledilmesi, bozulması, silinmesi, tahrip edilmesi, ortadan kaldırılması suretiyle seçimlik hareketleri ile gerçekleştirilebileceğini sonuçta sistemin işleyişinin engellendiğini belirtmekte ise de bu hareketler madde içerisinde suç tipinde düzenlenmediğinden seçimlik hareketten ziyade serbest hareket olarak değerlendirilmelidir. Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 190, 191.

fiile (harekete) ilişkin özel bir belirleme veya sınırlama yapılmamıştır.[1036] O halde, bilişim sistemini engelleyebilecek veya bozabilecek bir hareket ile bu suç işlenebileceğinden 244/1. m.'nin serbest hareketli bir suç olduğunu söyleyebilmekteyiz. Ayrınca doktrinde 244. m.'nin 1. fıkrasında yer alan suçun oluşumu açısından mağdur veya suçun konusunda ayrıca bir zararın oluşması aranmadığını belirten yazarlar[1037] da bulunmakta ise de kanaatimizce engelleme veya bozma bir zarar oluşturduğundan bu suç bir zarar suçudur.

3.2.2.2.3.1.1. Bilişim Sisteminin İşleyişini Engellemek

"Engelleme" ve "bozma" ifadelerine ilişkin olarak doktrinde farklı tanımlar bulunmaktadır. Engelleme fiilinin, sistemin gereği gibi çalışmasının önlenmesi, sistemin işleyişinin yavaşlatılması,[1038] veri işlem yapılmasını engellemeye yönelik her türlü hareket,[1039] sistemin olağan işleyişini durdurmak ve fonksiyonlarının doğru biçimde işlemesini engellemek,[1040] sistemin gerektiği gibi çalışmasının önlenmesi, işleyişinin yavaşlatılması veya tamamen kilitlenme noktasına gelmesi,[1041] sisteme etkide bulunularak sistemin düzgün işlemesinden elde edilecek her türlü faydanın engellenmesi,[1042] bilişim sisteminin işleyişini geçici olarak kesintiye uğratmak,[1043] sistemin işleyişinin geçici veya sürekli olarak çalışmasının herhangi bir şekilde

1036 "… 1. fıkrada yer alan hareketler her ne kadar suç tanımı açısından seçimlik hareketli olsalar da kendi içlerinde serbest hareketlidirler. Bir başka deyişle sistemin işleyişini bozma veya engelleme hareketlerinin nasıl yapıldığının tipiklik açısından bir önemi yoktur, suçun gerçekleşmesi için gerekli olan neticede sistemin işleyişinin engellenmesi veya bozulmasıdır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 332.
"Bu tür müdahalelerin ne şekilde gerçekleştirildiğinin bir önemi yoktur. Siber Suç Sözleşmesinin 5. maddesinin aksine, 244. maddenin ilk fıkrasında engellemenin hangi hareketlerle gerçekleştirilmesi gerektiği belirtilmemiştir." Bkz. Koca ve Üzülmez, a.g.e., s. 829.
"Suç birden fazla ve farklı hareketle gerçekleştirilebilir." Bkz. Soyaslan, a.g.e., s. 648.
1037 "Ancak yargıç, zararın oluşumunu 61. madde bağlamında temel cezadan uzaklaşıp üst sınıra yaklaşma açısından değerlendirebilir." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 332, 333.
1038 Mahmutoğlu, a.g.e., s. 866.
1039 Akbulut, *Bilişim Alanında Suçlar*, s. 190; Aynı yönde bkz. Özbek, v.d., a.g.e., s. 935.
Koca-Üzülmez de: "…Engelleme, bilişim sisteminin uygun şekilde işleyişine müdahale eden fiiller için kullanılmıştır. Bilişim sisteminin işleyişi, veri işleme faaliyeti anlamına gelmektedir." Bkz. Koca ve Üzülmez, a.g.e., s. 828.
1040 Eker, a.g.e., s. 125.
1041 Kurt, a.g.e., s. 161.
1042 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 320; Aynı yönde bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 216.
1043 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6928.
"…sistemin olağan işleyişini yavaşlatma da kanaatimizce engelleme olarak düşünülmelidir. Örneğin bilişim sistemine herhangi bir suretle sokulan ve sistemin işleyişini aşırı derecede zayıflatan "tavşan-rabbits" programlarının kullanımı da bu anlamda sistemin işleyişini engellemedir." Bkz. A.e.

kesintiye uğratılması,[1044] şeklinde tanımlandığı görülmektedir. AKSS' nin 5. m.'sine göre ise bilişim sisteminin işleyişinin engellenmesi, sisteme bilişim verilerinin girilmesi, nakledilmesi, bozulması, silinmesi, tahrip edilmesi, ortadan kaldırılması suretiyle gerçekleştirilebilmektedir.[1045] TDK sözlükte ise "engellemek", "Bir şeyin gerçekleşmesini veya yapılmasını önlemek"[1046] şeklinde tanımlanmıştır.

Doktrinde bazı yazarlar tarafından engellemenin geçici olması gerektiği[1047] bazı yazarlar tarafından ise engellemenin geçici veya sürekli olmasının bir etkisi olmadığı önemli olanın sistemin çalışmasının bir şekilde kesintiye uğratılması olduğu[1048] belirtilmektedir. Kanaatimizce de engellemenin süresi bakımından bir ayrıma gitmek doğru bir yaklaşım oluşturmayacaktır. Zira, kanunumuzda hem madde metninde hem de gerekçesinde böyle bir ayrıma gidilmemiş madde düzenlemesi ile engelleme neticesini doğurabilecek her türlü fiil ile suçun oluşacağı kabul edilmiştir. Bu doğrultuda, esasen teknik bir olgu olduğu da göz önünde bulundurularak engelleme veya bozma halinin şüpheye mahal bırakmayacak şekilde yine her somut olayda ayrıca değerlendirilerek sonuca varılması gerektiğini değerlendirmekteyiz.[1049]

Kanaatimizce, bilişim sisteminin işleyişinin engelleme neticesi, sistemin normal ve olağan zamanda sağlıklı bir şekilde yerine getirmekte olduğu fonksiyonların yerine getirilmemesi, işlevinin sekteye uğratılması veya aksatılması, buna sebep olan hareketin veya hareketlerin ortadan kalması halinde işlevine devam edebilecek olması anlamına gelmektedir. Nitekim, Erdoğan' ın da belirtmiş olduğu gibi bilişim sisteminin işleyişinin engellenmesi halinde sistemin bozulması söz konusu olmayıp normal şartlarda yerine getirdiği işlevlerini hiç veya gereği gibi yerine getirilememesi hali mevcuttur.[1050]

1044 Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 215.

1045 "Bu durumlarda sistemin bozulması söz konusu olmayıp normalde yerine getirdiği fonksiyonlarını ifa etmesi engellenmektedir." Bkz. Parlar ve Hatipoğlu, a.g.e., s. 3750.

1046 https://sozluk.gov.tr/, ET. 19 Mart 2020.

1047 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6928; Özbek, v.d., a.g.e., s. 936; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 219, 220; "Kanaatimizce engelleme geçici olmalıdır. Zira engelleme süreklilik taşırsa artık sistem gerektiği gibi faaliyet yapamadığından engellemenin ötesine geçilmiş olunmaktadır. Bu durumsa artık bozulma olarak nitelendirilmelidir." Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 190.

1048 Parlar ve Hatipoğlu, a.g.e., s. 3750; Soyaslan, a.g.e., s. 644; Yaşar, Gökcan ve Artuç, a.g.e., s. 7309; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 321; Akbulut, *Bilişim Alanında Suçlar*, s. 193.

1049 Aynı yönde bkz. Özbek, v.d., a.g.e., s. 936.

1050 "…Mesela sistem eskisi kadar hızlı çalışamamakta, veri alış verişi yapamamakta, veri işleme hızı düşmekte, istenilen performansta çalışamamakta, dosyaları açamamakta, çeşitli programları hiç, ya da gereği gibi çalıştıramamakta, kısacası normal şartlarda yerine getirebildiği işlevlerini ya hiç

Doktrinde fikir ayrılığı bulunan bir başka konu ise bilişim sisteminin işleyişinin engellemesi halinin sistemin soyut unsurlarına yönelik mi olacağı yoksa sistemin fiziki unsurlarına müdahalelerin de bu kapsamda değerlendirilip değerlendirilemeyeceğine ilişkindir. Koca-Üzülmez' e göre, suçun kanuni tanımında bilişim sisteminden değil bilişim sisteminin işleyişinin engellenmesinden ve bozulmasından bahsedildiği için suçun konusunu oluşturan sistemin işleyişini sağlayan soyut unsurlarına zarar verme fiili 244. m.'nin 1. fıkrası kapsamına girmekte, bilişim sisteminin maddi unsurlarına yönelik zarar verme niteliğindeki fiiller ise mala zarar verme suçunu oluşturmaktadır.[1051] Ancak bizim de katılmış olduğumuz diğer görüşe göre[1052], bilişim sisteminin işlenmesine engel olma fiziki etki şeklinde gerçekleşebileceği gibi soyut unsurlara yapılan müdahalelerle de gerçekleşebilecektir. Zira, bir bilişim sistemi hem soyut hem de fiziki unsurlardan oluşmakta olup fiziki unsurlarda gerçekleştirilecek hareketler de bilişim sisteminin işleyişinin engellenmesi sonucunu doğuruyor ise bu kapsamda kabul edilecektir.[1053] Zira, Akbulut' un da belirtmiş olduğu gibi 244. m.'nin

---

ya da gereği gibi yerine getirememektedir." Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 189.

Aynı yönde görüşe sahip Kurt örnek olarak: "Mesela sistem eskisi kadar hızlı çalışamamakta, veri alışverişi yapamamakta, veri işleme hızı düşmekte, istenilen performansta çalışamamakta, dosyaları açamamakta, çeşitli programları hiç, ya da gereği gibi çalıştıramamakta, kısacası normal şartlarda yerine getirebildiği işlevlerini ya hiç ya da gereği gibi yerine getirememektedir…" bkz. Kurt, a.g.e., s. 164.

1051 "…bir kimsenin diz üstü bilgisayarının yere fırlatılmak suretiyle parçalanması veya klavyenin tuşlarının sökülmesi halinde, bu fiilleri bilişim sisteminin işleyişinin engellenmesi veya bozulması olarak nitelendirmek mümkün değildir. Zira burada bilgisayar kişinin malvarlığında yer alan bir değer olarak tahrip edilmektedir. Aynı şekilde bir bilgisayarın klavyesinin, faresinin, içerisindeki bir parçanın tahrip edilmesi halinde de mala zarar verme suçu oluşacaktır. Buna karşılık bilgisayarın fiziki varlığına zarar vermeksizin gönderilen bir virüs programı ile çalışmaz hale getirilmesi durumunda, bilgisayar, malvarlığında bulunan bir değer olarak değil, bilişimi sağlayan bir araç olarak etkisiz kılınmaktadır…

…Bilişim sisteminin işleyişinin engellenmesi veya bozulması, sistemin donanım unsuruna verilen zararla yazılımın etkisiz kılınması halinde değil, yazılım unsuruna yönelik müdahale sonucu donanımın bir işe yaramaması halinde gerçekleştirilebilir…" bkz. Koca ve Üzülmez, a.g.e., s. 827-829.

Özbek vd.' leri de bilişim sistemi dışındaki unsurlara yapılan müdahalelerin 244. madde kapsamında engelleme veya bozma olarak kabul edilemeyeceğini belirtirken buna örnek olarak bilgisayarın yere atılarak kırılması, klavyenin tuşlarının parçalanmasını örnek vererek bu hallerde mala zarar verme suçunun oluşacağını belirtmektedirler. Bkz. Özbek, v.d., a.g.e., s. 936.

1052 "Engellemeyi sağlayacak her türlü hareket suçu oluşturabilir. Engel olma, bilişim sisteminin genel olarak işleyişine yönelik olabileceği gibi, bu işleyişe katkısı veya etkisi olan herhangi bir unsurun işleyişine engel olunarak da gerçekleşebilir; bu hâlde yeter ki bu unsurun işleyişine engel olunması sistemin işleyişini kısmen veya tamamen engellemiş olsun." Bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 216.

Aynı yönde görüş için bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6928.

1053 "Burada korunmak istenen sadece verilere müdahale edilmeden sistemin usulüne uygun çalışması değil, herhangi bir problem olmadan sistemin çalışmasındaki yarardır. Dolayısıyla yalnızca soyut unsurlara müdahaleyle bunun sağlanamayacağını düşünüyoruz." Bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 192.

AKSS' de karşılığı olan 5. m.'de yer alan sadece sistemin soyut unsurlarına müdahale edilmek suretiyle işleyişin engellenmesine yönelik sınırlama da 244. m.'nin 1. fıkrasında yer almamaktadır.[1054] Bu bağlamda, sistemin işleyişinin engellenmesi, elektriğin kesilmesi, sistemleri birbirine bağlayan kabloların çıkarılması, bilişim sisteminin donanımına ait bir unsurun çıkarılması gibi somut unsurlara yönelik olabileceği gibi zararlı bir yazılımın bulaştırılması, sisteme yöneltilecek yoğun elektromanyetik dalgalarla sistem merkezinin etkilenmesi veya DoS veya DDoS saldırıları gibi soyut unsurlara yönelik hareketlerle de gerçekleştirilebilmektedir.[1055] Ancak burada belirtmek gerekir ki Dülger' in de belirtmiş olduğu gibi 151. m. ile 244.

Yargıtay 11. Ceza Dairesi'nin konuya ilişkin vermiş olduğu 7.3.2012 tarili, E.15938, K.3094 sayılı kararında:
'5237 sayılı TCK'nun 244. maddenin 1. fıkrasında "bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması," fiilleri suç olarak düzenlenmek suretiyle Avrupa Siber Sözleşmesi'ne paralellik sağlamak amacıyla bir bilişim sisteminin işleyişinin "engellenmesi veya "bozulması" bir yarar sağlama koşuluna bağlanmaksızın bağımsız suç olarak düzenlenmiştir. Sistemin işleyişinin "engellenmesi" ibaresi ile bilişim sisteminin verimli çalışmasının önlenmesi, icra ettiği faaliyet ve sahip olduğu kapasitesinin müdahale ile sınırlandırılması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi, sistemin "bozulması" tabiri ile ise; bilişim sistemine dahil olan mekanik parçanın veya bir yazılım programının esasen yapması gereken özgülendiği işlevi yapamayacak hale getirilmesi ile birlikte sistemin engellenmesi halinin en üst noktası olan durma noktasından daha ileri olarak sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi, hatta fiziki olarak dahi zarar verilmesi anlaşılmalıdır. Madde gerekçesinde de belirtildiği üzere söz konusu madde ile bilişim sistemlerine yöneltilen ızrar fiilleri seçimlik hareketli özel bir suç haline getirilmiş olup, bilişim sisteminin fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır.
Somut olayda; yapılan ihbar üzerine emniyet görevlilerinin suça konu … Bankası'na ait ATM'de tertibat aldıktan sonra kendilerine ait bankamatik kartını vererek gönderdikleri elemanın para çekmek için uğraştığı sırada yanına gelen sanıkların önceden ATM'nin kart yuvasına taktıkları aparat ile kurdukları düzenek sayesinde kartın sıkışmasını sağladıktan ve yardım bahanesiyle şifresini öğrendikten sonra ele geçirdikleri bankamatik kartı ile uzaklaşmak istedikleri sırada yakalanmaları şeklinde gerçekleşen eylemlerinin; kartın sıkışmasını sağlamak için yerleştirilen aparatın takılı olduğu süre boyunca bilişim sisteminin bir parçası olan ATM'nin kullanılamaması, şikayetçi banka görevlisinin 01.08.2005 günlü ifadesinde suça konu ATM'nin kart girişinde bulunan muhafaza plastik kısmının kesici bir aletle kesildiği ve şikayetçi olduklarını belirtmesi karşısında; gerçeğin ve suç niteliğinin kuşkuya yer vermeyecek şekilde belirlenebilmesi ve sanığın/sanıkların bilişim sisteminin parçası olan ATM üzerinde gerçekleştirdikleri hareket/hareketlerinin ayrıntılı olarak tespiti ile bu hareketin suça konu bankanın bilişim sisteminin bir parçası olarak tespiti ile bu hareketin suça konu bankanın bilişim sisteminin bir parçası olan ATM'nin kısa süreliğine de olsa çalışmasına engel teşkil edip etmediği, bağlı bulunduğu bilişim sistemine (sistemin engellenmesi veya bozulması gibi) bir zarar verip vermediği hususları araştırılarak ilgili banka şubesinden sorulup, gerektiğinde uzman bir bilirkişiden rapor alınıp, ATM'nin ait olduğu bankanın şikayetçi olduğu hususu da dikkate alınmak suretiyle sanık/sanıkların eylemlerinin "bilişim sistemini engelleme veya bozma" suçunu mu yoksa "mala zarar verme" suçunu mu oluşturduğu karar yerinde tartışılarak hukuki durumunun/durumlarının takdir ve tayini gerektiği gözetilmeyerek eksik soruşturma ve suç vasfında yanılgı sonucu yazılı şekilde "banka veya kredi kartlarının kötüye kullanılmasına teşebbüs" suçunu oluşturacağından bahisle yazılı şekilde hüküm kurulması, Yasaya aykırıdır' şeklinde karar verilmiştir. (*Aktaran* Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 227, 228).
1054 Bkz. *Akbulut, Bilişim Alanında Suçlar*, s. 192.
1055 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 321; Soyaslan, a.g.e., s. 644; Mahmutoğlu, a.g.e., s. 866; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 219; Özbek, v.d., a.g.e., s. 936; Parlar ve Hatipoğlu, a.g.e., s. 3750.

m.'nin 1. fıkrası birbirinden tamamen farklı iki suç tipini düzenlemekte olup salt mala zarar verme kastıyla yapılan bir eyleme 151. m.'nin uygulanması gerekirken 244. m.'nin gerekçesinde "ızrar" yazıyor diye bu madde uygulanmamalıdır.[1056] Dolayısıyla fiilin niteliğinin tayininde failin kastı gözetilmelidir.[1057]

Son olarak değinmek istediğimiz husus ise bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu ile bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi suçunun birlikte gerçekleşmesi halinde çözümün nasıl olacağıdır. Doktrinde yer alan bir görüşe göre bilişim sisteminin engellenmesi veya bozulması sistem içerisinde yer alan verilere müdahale şeklinde gerçekleşirse, bu tür müdahalelerin sistemin işleyişini engellemedikçe veya bozmadıkça 244. m.'nin 2. fıkrasındaki suçu oluşturacağı, sistemin işleyişini engellemesi veya bozması halinde ise 244. m.'nin 1. fıkrasında yer alan suçun oluşacağıdır.[1058] Doktrinde yer alan bir diğer görüşe göre ise, böyle bir durumun varlığı halinde tek fiil ile farklı suçlar gerçekleştiğinden sorun TCK m. 44 fikri içtima hükümlerine göre çözümlenmelidir.[1059] Bir başka görüşe göre ise böyle bir durumun varlığı halinde failin

1056 "…çünkü maddelerin gerekçelerinde suç tipini oluşturan eylemlerin ya da suçun konusunu oluşturan nesnelerin belirlenmesi mümkün değildir." Bkz. Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 338. Aynı yönde bkz. Soyaslan, a.g.e., s. 650.

151. madde ile 244. madde arasındaki ilişki için ikinci fıkra açısından da aynı görüşe katılmaktayız. Ancak bu konuda Artuk, Gökcen ve Yenidünya: "Bilişim sistemindeki verilere zarar verilmesi, TCK.'nın 151 inci maddesinde yer alan mala zarar verme suçunu da oluşturmaktadır. Bu ihtimalde farklı neviden fikri içtimaa ilişkin 44 üncü madde uyarınca bir sonuca ulaşılması yerinde olur." Fikrini taşımaktadır. Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6936. Aynı yönde bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 210, 211.

Ancak Erdoğan ise verinin mal olmadığı, verilere zarar verilmesi halinde suçta ve cezada kanunilik ilkesi ve kıyas yasağı nedeniyle 151. maddenin uygulanmasının imkanı bulunmadığı, zira kanunkoyucunun da bu noktada verilere zarar verilmesini yaptırımsız bırakmamak için 2. fıkra düzenlemesini yaptığı, bu düzenlemenin klasik mala zarar verme suçunun bilişim alanındaki karşılığı olduğunu belirtmektedir. Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 237.

1057 Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 228.

1058 Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6929; Koca ve Üzülmez, a.g.e., s. 829; Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 217, 218; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 332.

1059 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 236; Akbulut, *Bilişim Alanında Suçlar*, s. 210.

Akbulut ayrıca, 765 sayılı TCK'nın 525/b-1 maddesinde yer alan tahrip etme seçimlik hareketini değerlendirirken verilere zarar vermeyen hareketlerin tahrip etme olarak kabul edilemeyeceğini, bu hareketlerin sisteme engel olma olarak nitelendirilebileceği, tahrip edilmenin ayrıca düzenlenmesine gerek olmadığı, tahriple verilerde bir zarar oluşmuşsa bunun zaten verilerin tahrip edilmesi kavramına gireceği, verilere bir zarar verilmesinin söz konusu olmayıp sistemin işleyişine engel olunmuşsa bunun sisteme engel olma kavramı içinde değerlendirileceğini, her ikisi de söz konusu değilse mala zarar verme suçunun oluşacağını belirtmektedir. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 193.

kastı dikkate alınmak suretiyle oluşan suç belirlenmelidir.[1060] Yargıtay' ın da konu ile ilgili genel yaklaşımı ise belirtmiş olduğumuz birinci görüş yönünde[1061] ise de Yargıtay 23. Ceza Dairesi ise bir kararında:

> "*Sanık hakkında bilişim sistemindeki verileri bozma suçundan verilen hükmün temyiz incelemesinde;*
>
> *Sanığın katılan ...'a ait "facebook" hesabındaki verilere yönelik bozma veya değiştirme gibi bir eylemde bulunmadan bu hesaba dair şifreyi değiştirip hesap sahibi gibi hareket etmek şeklinde gerçekleştirdiği eyleminin TCK'nın 244/1. maddesindeki bilişim sisteminin işleyişini engelleme suçunu oluşturduğu gözetilmeden sanık hakkında TCK'nın 244/2. maddesi gereğince uygulama yapılması, ... BOZULMASINA,"*[1062]

1060 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 321; Soyaslan, a.g.e., s. 644; Kurt, a.g.e., s. 167.

1061 Yargıtay 8. Ceza Dairesi vermiş olduğu bir kararda:
"…Sanığın, şikayetçiye ait MSN adresini ve şifresini ele geçirdikten sonra şikayetçinin hesabına girip şifresini değiştirdiğinin iddia olunması karşısında; suça konu eylemin TCK'nın 244/2. maddesinde düzenlenen suçu oluşturup oluşturmayacağına iliş- kin delilleri takdir ve tartışmanın 5235 sayılı Yasanın 11. maddesi uyarınca Asliye Ceza Mahkemesinin görevi kapsamında bulunduğu gözetilerek görevsizlik kararı verilmesi gerekirken, yargılamaya devamla yazılı şekilde hüküm kurulması, … (BOZULMASINA)" hususlarına yer vermiştir. Bkz. Yargıtay 8. Ceza Dairesi, 16.3.2015 t., E:2014/33504, K:2015/13751, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yargıtay 15. Ceza Dairesi, 18.5.2016 tarihli bir kararında: "…Mağdura ait elektronik postaya bağlı facebook hesabının şifresini ele geçirerek bu adrese giren, yazışmalar yapan ve şifreyi değiştirmek suretiyle mağdurun anılan hesaba erişimini engelleyen sanığın eyleminin, 5237 Sayılı TCK'nın 244/2. maddesinde düzenlenen suçu oluşturacağı gözetilmeden suç vasfında hataya düşülerek yazılı şekilde hüküm kurulması," şeklinde karar vermiştir. Bkz. Yargıtay 15. Ceza Dairesi, 18.5.2016 t., E: 2013/32575, K: 2016/5124, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay 12. Ceza Dairesi' nin 22/12/2014 tarihli bir kararında: "…Sanığın, mağdur ...'in, e-posta adresi ve şifresi ile facebook hesabı için yeni şifre oluşturarak hesabına girmesi, hesaba fotoğraf yerleştirdikten sonra e-posta adresi ve facebook hesabının şifrelerini değiştirerek mağdurun hesaplara erişimine engel olması biçimindeki eyleminin, TCK'nın 244/2. maddesine uygun bulunduğu gözetilmeden, olayda uygulama yeri bulunmayan aynı Kanunun 244/1. maddesi uyarınca hüküm kurulması, Kanuna aykırı,", bkz. Yargıtay 12. Ceza Dairesi, 22/12/2014 t., E:2014/10843, K:2014/26243, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yargıtay, 8. Ceza Dairesi 24.6.2014 tarihli bir kararında da: "Katılana ait hotmail adresine hukuka aykırı olarak giren ve yeni şifre oluşturup katılanın erişimini engelleyerek e-mail adresini kullanan sanığın eylemine uyan TCK. nun 244/2. madde ve fıkrası uyarınca cezalandırılması gerektiği gözetilmeden yazılı şekilde yasal ve yeterli olmayan gerekçeyle beraatına hükmolunması, … BOZULMASINA," hükmetmiştir. Bkz. Yargıtay, 8. Ceza Dairesi 24.6.2014 t., E: 2013/771, K: 2014/15833, https://legalbank.net/arama, ET. 15 Temmuz 2020. Aynı yönde bkz. Yargıtay 8. CD., 24.6.2013 t., E: 2012/32866, K: 2013/18872.

1062 Bkz. Yargıtay 23. Ceza Dairesi, 24.5.2016 t., E: 2015/9146, K: 2016/6542, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay 8. Ceza Dairesi' nin kanaatimizce yanlış nitelendirmede bulunduğu 12.11.2015 tarihli, E: 2015/5648, K: 24511 sayılı kararında: "İddianamedeki anlatıma göre, sanık hakkında katılan adına ve fotoğrafını kullanarak … isimli sosyal paylaşım sitesinde hesap oluşturduğu ve katılanın arkadaşlarına hakaret ettiği iddiası ile TCK'nın 136/1, 53. maddeleri uyarınca cezalandırılmasının istenmesine karşın, mahkumiyet hükmünün katılanın sosyal medya hesabının şifresini ele geçirip değiştirerek bilişim sistemini bozduğuna veya erişilmez kıldığına yönelik olması ve TCK.nun 244/2, 53. maddeleri uyarınca mahkumiyet hükmü kurulması suretiyle 5271 sayılı CMK'nın 225. maddesine aykırı davranılması, … (BOZULMASINA)" karar verilmiştir. Bkz. https://legalbank.net/arama, ET. 15 Temmuz 2020.

şeklinde karar verilmişse de kanaatimizce bu karar hatalıdır. Zira, 244. m.'nin 1. fıkrasında yer alan suçun koruduğu hukuksal değer açıklanırken de belirtmiş olduğumuz üzere bu suç ile korunan değerlerden bir tanesi bilişim sisteminin güvenliğidir. Suç tipinde yaptırım altına alınan hal ise bilişim sisteminin işleyişinin engellenmesi veya bozulmasıdır. Kararda sanık tarafından gerçekleştirilen eylem ise şifrenin değiştirilmesi yani bir başka deyişle sistemin soyut unsuru olan verileri erişilmez kılmak suretiyle sisteme erişimin engellenmesini ifade etmektedir. Bilişim sisteminin işleyişinin engellenmesinden kasıt ise olağan fonksiyonlarını ve normal işlevini yerine getirememesidir. Kararda belirtilen durumda ise normal işleyişine devam etmekte olan bir bilişim sistemindeki verilerin bir başkası tarafından erişilmez kılınması söz konusudur. Kaldı ki, aksi görüş 244. m.'nin 2. fıkrasında ayrıca düzenlenmiş olan suçu gereksiz kılacaktır. Bu sebeple esasen burada bir bilişim sisteminin işleyişinin engellenmesi değil verilerin erişilmez kılınması suretiyle bilişim sistemine erişimin engellenmesi söz konusu olduğundan bu ve benzer durumlarda 244. m.'nin 2. fıkrasında yer alan suçun uygulanması yerinde olacaktır. Bunun yanında Yargıtay, bilişim sisteminin işleyişini engellemek veya bozmak suçundan açılmış olan birçok davada, bilirkişi incelemesi yaptırılıp sonucuna göre değerlendirme yapılması gerektiğinin gözetilmediği, eksik inceleme yapıldığından bahisle bozma kararları vermektedir.[1063]

Kanaatimizce, bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu ile bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi suçlarının birlikte gerçekleşmesi halinde failin kastının dikkate alınması muhakkaktır ki önem arz etmektedir. Ancak 1. ve 2. fıkra kapsamında yer alan suçların olası kastla da işlenebilmesi mümkün olduğundan, verilere müdahale kastı ile hareket

1063 "Şikayetçi vekillerinin, şirkete ait internet sitesine dışarıdan yapılan bir müdahale ile erişimin sağlanamadığını şikayetçi olması üzerine başlatılan soruşturma neticesinde, şikayetçi vekili tarafından sunulan IP bilgisinin kim tarafından kullanıldığına ilişkin talebin mahkemece reddedilmesi üzerine başkaca bir araştırma yapılmaksızın, iddiadan öte kamu davası açmaya yeterli delil elde edilemeyeceğinden bahisle kovuşturmaya yer olmadığına dair karar verildiği ve verilen bu karara karşı yapılan itirazın, mercii tarafından reddedilmesi üzerine kararın kesinleştiği anlaşılmıştır…
…İncelemeye konu olayda, şikayeti üzerine ilgili internet sitesi ve sisteminde bilirkişi incelemesi yaptırılıp eylemi gerçekleştiren kişilerin gerektiğinde erişim sağlayıcıdan kimlik bilgileri de sorulmak suretiyle sonucuna göre değerlendirme yapılması gerektiği gözetilerek itirazın kabulüne karar verilmesi gerekirken, yazılı şekilde reddine karar verilmesi, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 7.3.2016 t., E: 2016/804, K: 2016/2811. Bkz. https://legalbank.net/arama, ET. 15 Temmuz 2020.
Aynı yönde bkz. Yargıtay 8. Ceza Dairesi, 16.4.2014 t., E: 2013/4668, K: 2014/9860.

eden failin de genelde sistemin engellenmesi veya bozulması açısından olası kastı bulunabileceğinden[1064] başka bir deyişle sistemin engellenmesi veya bozulması suçu olası kastla da işlenebileceğinden[1065] burada failin kastının esas alınmak suretiyle bir ayrıma gidilmesi ve çözüme ulaşılması zor görünmektedir. Dolayısıyla, böyle bir durumun varlığı halinde tek fiil ile birden fazla farklı suçun işlenmesi söz konusu olacağından ikinci görüşte belirtildiği gibi sorunun fikri içtima kuralları uyarınca çözülmesi gerektiğini değerlendirmekteyiz. O halde fail daha ağır ceza öngören 1. fıkra kapsamında cezalandırılacaktır.

3.2.2.2.3.1.2. Bilişim Sisteminin İşleyişini Bozmak

TDK Sözlükte, "Bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek", "Geçersiz bir duruma getirmek"[1066] olarak tanımlanan "bozmak" ifadesi için bilişim sisteminin bozulması kavramı için doktrinde bilişim sisteminin kısmen veya tamamen işleyemez hale getirilmesi,[1067] verileri aktarmasının sistemden beklenildiği şekilde gerçekleştiremeyecek, eskisi gibi yapamayacak hale getirilmesi,[1068] veri işleme faaliyeti yapamayacak hale getirilmesi ya da doğru sonuçlara ulaşmasına engel olacak şekilde müdahalede bulunulması,[1069] sistemden kalıcı surette sistemden istifadenin engellenmesi,[1070] haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan kaldırılması,[1071] kendisinden beklenilen işi yapamayacak duruma getirilmesi,[1072] sistemin hiçbir fonksiyonunu

1064 Aynı yönde bkz. Karagöz, a.g.e., s. 142.
1065 "Başkasının sistemine girip sisteme ilişkin verilerini tahrip eden kişi pekala bu arada sisteminde zarar görebileceğini bilmekte, buna rağmen eylemine devam etmektedir. Dolayısıyla olası kasttan dolayı da ağır cezayı içeren, birinci fıkranın tatbik edileceğini düşünmekteyiz." Bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 236.
1066 https://sozluk.gov.tr/, ET. 23 Mart 2020.
1067 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 321.
Özbek vd.' ne göre de: "…dışarıdan gerçekleştirilen bir müdahale ile … kendisinden beklenen işi yapamayacak şekilde kısmen veya tamamen tahrip edilmesi durumu da "bozma" olarak kabul edilmelidir." Bkz. Özbek, v.d., a.g.e., s. 935.
Aynı yönde bkz. Mahmutoğlu, a.g.e., s. 867.
1068 Akbulut, *Bilişim Alanında Suçlar*, s. 194.
1069 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 193.
1070 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6929.
1071 Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 231.
1072 Soyaslan, a.g.e., s. 644.
Soyaslan' a göre verileri içeren bilişim sistemi ya da veri taşıma aracının kısmen veya tamamen bozulması açısından bir fark bulunmamaktadır. Ancak kısmen bozma eyleminin gerçekleşebilmesi için bozulan kısım nedeniyle bilişim sistemi içinde bulunan verilerin bir daha kullanılamaz hale gelmesi gerekmektedir. Bkz. A.e.

yerine getiremediği kronik bir çalışamama,[1073] tanımlarına yer verilmiştir. Yargıtay' a göre bilişim sisteminin işleyişinin bozulması, *'bilişim sistemine dâhil olan mekanik parçanın veya bir yazılım programının esasen yapması gereken özgülendiği işlevi yapamayacak hale getirilmesi ile birlikte sistemin engellenmesi halinin en üst noktası olan durma noktasından daha ileri olarak sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi veya fiziki olarak dahi zarar verilmesi olarak anlaşılmalıdır.'*[1074]

Kanaatimizce de bilişim sisteminin bozulması, sistemin normal ve olağan işlevinin yerine getirilmesinin ortadan kaldırılması başka bir deyişle sistemin kullanılamaz hale getirilmesi[1075] anlamına gelmekte olup bilişim sisteminin engellenmesi halinde belirtmiş olduğumuz gibi bu halin gerçekleşmesi bakımından müdahalenin sistemin fiziki veya soyut unsurlarına yönelik olarak gerçekleştirilmesi bakımından her somut olayın özelliği ayrıca göz önünde bulundurulmak koşuluyla bir fark bulunmamaktadır. Bunun yanında bilişim sistemini bozmaya yol açacak eylemin nasıl gerçekleştirildiğinin de suçun oluşumu açısından bir önemi bulunmamaktadır.[1076]

3.2.2.2.3.2. Bilişim Sisteminde Yer Alan Verileri Bozmak, Yok Etmek, Değiştirmek, Erişilmez Kılmak, Sisteme Veri Yerleştirmek veya Var Olan Verileri Başka Yere Göndermek

244. m.' nin 2. fıkrasında düzenlenmiş olan suçun fiil unsuru bilişim sistemindeki verinin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, bilişim sistemine veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi seçimlik hareketlerinden birinin gerçekleştirilmesiyle oluşacaktır.[1077] Somut olayda birden fazla hareketin birlikte gerçekleştirilmesi halinde ise bu durum ceza tayininde

1073 Eker, a.g.e., s. 125.
1074 'Yargıtay 11. CD., 13.3.2013 t., E: 2011/2816, K: 2013/4065' (*Aktaran* Akbulut, *Bilişim Alanında Suçlar*, s. 194).
1075 'Yargıtay 8. Ceza Dairesi' nin 4.10.2017 tarihli E: 2016/8701, K: 2017/ 10869 sayılı kararı ile: 'daha önce çalıştığı firmada internet üzerinden kullanılan A… isimli eğitim programının bildiği şifrelerini kullanarak bu programı kullanılamaz hale getiren sanığın, TCK'nın 244/1. maddesinde tanımlanan bir bilişim sisteminin işleyişini engelleme veya bozma fiilini gerçekleştirme eyleminden cezalandırılması' şeklindeki mahkeme kararı yerine bulunmuştur.' (*Aktaran* Gül, a.g.e., s. 89).
1076 Soyaslan, a.g.e., s. 644.
1077 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345, s. 6933*; Yaşar, Gökcan ve Artuç, a.g.e., s. 7311.

dikkate alınacaktır.[1078] Ancak burada belirtmek gerekir ki verilerin bozulması[1079], yok edilmesi, erişilmez kılınması, değiştirilmesi fiilleri sonucu veriye müdahale edecek nitelikte bir hareketle gerçekleşen bir netice aranmaktadır.[1080] Doktrinde bu suçun bağlı hareketli suç olduğunu belirten yazarlar[1081] bulunmakta ise de kanaatimizce madde metninde yaptırıma bağlanan hareketlerin (verileri bozmak, yok etmek, değiştirmek, erişilmez kılmak, sisteme veri yerleştirmek veya var olan verileri başka yere göndermek) işleniş biçimleri çeşitli yollarla gerçekleştirilebileceğinden ve esasen bu hareketlerin nasıl gerçekleştirileceği madde içerisinde gösterilmediğinden[1082] burada serbest hareketli bir suç söz konusudur. 244. m.'nin 1. fıkrası için belirtmiş olduğumuz gibi 2. fıkra açısından da bu madde metninde yer alan eylemlerin niteliği gereği zarar verici nitelikte olduğu suçun oluşumu açısından veriler üzerinde hak sahibi olan kişiler açısından ayrıca bir zararın oluşması şartının aranmadığı belirtilmekte ise de[1083] bu fıkra açısından sisteme yeni veri yerleştirme hususu dışında bir zarar suçu olduğu değerlendirilmektedir.[1084]

Yargıtay' ın bu suç kapsamında vermiş olduğu birçok kararda, bilişim sistemindeki verilerin bozulup bozulmadığı, yok edilip edilmediği, değiştirilip değiştirilmediği veya erişilmez kılınıp kılınmadığı, sisteme veri yerleştirilip yerleştirilmediği, var olan verilerin başka bir yere gönderilip gönderilmediği hususlarının net bir şekilde belirlenmesi gerektiği fikrinde olduğu görülmekte olup bu hareketlerin tespiti açısından eksik inceleme gerçekleştirildiğinden bahisle ilk derece mahkemesi kararlarının bozulmasına hükmettiği görülmektedir.[1085]

1078 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6933.

1079 Akbulut' a göre de: "Verilerin bozulması, verilerin kullanılabilirliğine zarar verilmesidir. Fıkrada kullanılan verilerin bozulması kavramı, bir neticeyi ifade etmektedir." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 195.

1080 Aynı yönde bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 332.

1081 Yaşar, Gökcan ve Artuç, a.g.e., s. 7314, 7321.

"…suçun oluşması için failin bilişim sistemindeki verileri bozması, yok etmesi, değiştirmesi, erişilmez kılması, sisteme veri yerleştirmesi veya var olan veriyi başka bir yere göndermesi gerekir, bunlar dışında bir harekette bulunduğunda anılan suç oluşmayacaktır." Bkz. A.e., s. 7321.

1082 Aynı yönde bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 332.

1083 "Ancak yargıç, zararın oluşumunu 61. madde bağlamında temel cezadan uzaklaşıp üst sınıra yaklaşma açısından değerlendirebilir." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 332, 333.

1084 Yaşar,Gökcan ve Artuç' a göre de: "Maddede belirtilen suç, yalnızca sisteme yeni veri yerleştirme hususu dışında bir zarar suçudur, sisteme yeni veri yerleştirme ise bir tehlike suçudur, veri yerleştirilince suç tamamlanır, ayrıca yeni verinin sisteme zarar vermesine gerek yoktur." Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7314.

Yine Yılmaz' a göre de: "TCK 244 maddesinde failin yaptığı hareketler neticesinde bir zarar meydana gelmesi aranmaktadır. Zaten bu eylemler neticesinde zararın meydana gelmemesi hayatın olağan akışına aykırıdır." Bkz. Yılmaz, a.g.e., s. 77.

1085 Katılanın yetkilisi olduğu otelin eski çalışanı olan sanık hakkında işten çıktıktan sonra kendisinde bulunan şifre ile daha önce çalıştığı otelin oda fiyatlarını düşürdüğü, bu şekilde 25 odanın

3.2.2.2.3.2.1. Verileri Bozmak

Verilerin bozulması, doktrinde bilişim sisteminde yer alan verinin yok edilmeden kendisinden beklenilen faydayı sağlayamayacak hale getirilmesi, verinin içeriğine ve yapısına müdahale etmek suretiyle kı smen veya tamamen kullanılamaz hale getirilmesi,[1086] verilerin belirlenen amaç doğrultusunda kullanılmasının tamamen veya kısmen ortadan kaldırılmasını sağlayacak şekilde zarar verilmesi,[1087] şeklinde tanımlanmakta olup esasen bilişim sistemini bozma başlığı altında yapmış olduğumuz açıklamalar verileri bozma fiili için de geçerlidir.

---

satışının gerçekleştiğinden bahisle açılan ve bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, sisteme veri yerleştirme suçundan yargılama yapılan bir davada: "Katılanın otel yetkilisi olduğu, sanığın da suç tarihinde bu otelde çalıştığı, otelin internetten oda satışı ile ilgili ... isimli internet sitesi ile anlaşmasının bulunduğu, otel görevlilerinin kendilerine verilen şifre ile bu siteye girerek otelin oda fiyatlarını güncelleyebildikleri, sanığın da otelde ön büro müdürü olarak çalışması nedeniyle bu şifrenin kendisinde de bulunup şikayet tarihi olan 05.05.2012 tarihinden yaklaşık 10 gün kadar önce buradaki işinden ayrıldığı, suç tarihinde ... ilçesinde faaliyet gösteren ... isimli otelde bir süre çalıştığı, bu otelde kurulu bulunan IP numaralı bilgisayardan 03.05.2012 tarihinde internete girerek daha önce çalıştığı otelin oda fiyatlarını düşürdüğü, bu şekilde 25 odanın satışının gerçekleştiğinden bahisle açılan davada, katılanın şikayet dilekçesi ekinde ibraz ettiği deliller dışında delil toplanmamıştır. Katılanın ve sanığın kullandığı bilgisayarlara el konulup hard disklerinin, suç tarihine ilişkin LOG kayıtları bakımından karşılıklı olarak incelenmesi, suç tarihinde bilişim sistemindeki verilerin bozulup bozulmadığı, yok edilip edilmediği, değiştirilip değiştirilmediği veya erişilmez kılınıp kılınmadığı, sisteme veri yerleştirilip yerleştirilmediği, var olan verilerin başka bir yere gönderilip gönderilmediği, nereye gönderildiği saptanıp, oda satışının yapıldığı internet sitesinden, satışın yapıldığı sıradaki IP numaralarının tespiti ile sonucuna göre, toplanan deliller değerlendirilerek sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, … (BOZULMASINA)" karar vermiştir. Bkz. Yargıtay 8. Ceza Dairesi, 11.1.2017 t., E: 2016/8498, K: 2017/175, https://legalbank.net/arama, ET. 15 Temmuz 2020.

Yine, katılanın kullandığı e-posta adresi ile irtibatlı olan facebook adresini bilgisi ve rızası olmaksızın değiştirerek erişilmez kılındığından bahisle açılan bir davada: "Somut olayda; sanığın, katılanın kullandığı "...@hotmail.com" e-posta adresi ile irtibatlı olan facebook adresine bilgisi ve rızası olmaksızın değiştirerek erişilmez kıldığından bahisle açılan davada, yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan mahkumiyet hükmü kurulmuştur. Sanığın suçlamayı kabul etmediği gibi hattına başkalarının girmiş olabileceği savunmasına ilişkin olmak üzere internet hattını sanık dışında başkalarının da kullanıp kullanmadığı ve kendisine ait olduğu belirtilen e-mail adresinin sanığa aidiyeti hususunda dosyada bir bilgiye rastlanmamıştır. Katılanın 27.05.2011 tarihinden itibaren e-mail adresine giremediğini belirttiğinin anlaşılması karşısında, anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, katılan tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit edilmemiştir. Sanık tarafından 22.05.2011 tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulmadan hüküm kurulmuştur.

Bu itibarla; yukarıda açıklanan yöntem izlenerek eksiklikler yerine getirilip sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, katılanın beyanına itibar edilerek ve eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, … BOZULMASINA," bkz. Yargıtay 8. Ceza Dairesi, 3.2.2015 t., E: 2014/19342, K: 2015/2322, https://legalbank.net/arama, ET. 15 Temmuz 2020.

Aynı yönde bkz. Yargıtay 8. Ceza Dairesi, 8.3.2018 t., E: 2018/1078, K: 2018/2485.

1086 Yaşar, Gökcan ve Artuç, a.g.e., s. 7311. Aynı yönde bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6933; Koca ve Üzülmez, a.g.e., s. 829; Özbek, v.d., a.g.e., s. 938.

1087 Akbulut, *Bilişim Alanında Suçlar,* s. 195, 196.

244. m.'nin 1. fıkrasında yer alan bilişim sisteminin işleyişinin bozulması fiili verilerin bozulması suretiyle de gerçekleştirilebilmekte olduğundan böyle bir durumun varlığı halinde failin kastı dikkate alınmak suretiyle oluşan suçun belirlenmesi gerektiğini belirten yazarlar[1088] bulunduğu gibi 2. fıkradaki suçun oluşabilmesi için bilişim sisteminin işleyişini etkilemeyecek verilere müdahale edilmesi gerektiğini, sistemin işleyişini etkileyecek verilere müdahalede halinde ise 1. fıkranın uygulanması gerektiğini belirten yazarlar[1089] da bulunmaktadır. Kanaatimizce, ilgili başlık altında da belirtmiş olduğumuz üzere böyle bir durumun varlığı halinde her iki suç da oluşacak olup tek fiil ile birden fazla suçun oluşumu söz konusu olduğundan sorun fikri içtima kurallarına göre çözülmelidir.

3.2.2.2.3.2.2. Verileri Yok Etmek

Ortadan kaldırmak anlamı bulunan[1090] yok etmek ifadesi üzerine doktrinde bilişim sistemlerinde bulunan verileri tamamen ortadan kaldırmak veya yok etmek mümkün olmadığından bilişim alanında geçerli olan soyut anlamda mantıksal yok etme fiilinin kastedildiği[1091] belirtilerek verileri yok etmek fiilinden anlaşılması

1088 Bkz. Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 167; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 321; Soyaslan, a.g.e., s. 644.
"Bilişim sisteminin işletim yazılımındaki sistem dosyalarını silmiş olan bir sanığın kastının, her olayın kendine has özellikleri de göz önüne alınmakla birlikte sadece verileri bozmak değil sistemin işleyişini bozmak olduğu kabul edilmelidir. Çünkü sıradan verilere değil, sistemin işleyişini sağlayan dosyalara yönelinmiştir." Bkz. Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 167.
1089 Erdoğan' a göre ikinci fıkra kapsamında korunan veriler bilişim sisteminin işleyişine ilişkin olmayan başka bir deyişle bilişim sistemi içinde yer alan ancak sistemin yapı taşı olmayan verilerdir. Bilişim sisteminin işleyişini etkileyecek verilere müdahalede 1. fıkra uygulanmalıdır. Bkz. *Erdoğan, Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 215.
1090 https://sozluk.gov.tr/, ET. 23 Mart 2020.
1091 Soyaslan, a.g.e., s. 645.
Ancak Parlar ve Hatipoğlu'na göre: " "Verilerin yok edilmesi", verilerin tamamen ortadan kaldırılması, varlığına son verilmesi anlamına gelmektedir. Bozulan verilerin onarılması mümkün olduğu halde, yok edilen verilerin sağlıklı hale getirilmesi mümkün değildir. Bilgisayar temelli yollarla verilerin tamamen silinmesi (yok edilmesi) mümkün değildir. Verilerin yok edilmesi sadece fiziki müdahalelerle mümkün olmaktadır. Örneğin, verilerin bir taşıma aracında bulunduğu durumda (hard disk, disket, CD, USB cihazı vs.) aracın yakılmasıyla verilerin yok olması durumunda bu suç oluşacaktır." Bkz. Parlar ve Hatipoğlu, a.g.e., s. 3751.
Akbulut' a göre de verilerin yok edilmesi: "Bilişim sisteminde depolanmış verilerin tamamen ve telafisi olmayacak şekilde tanınmaz hale getirilmesidir." olup veriler için "…geri getirme imkânı varsa verilerin yok edilmesinin söz konusu olmadığını ifade ediyoruz." şeklinde belirtmiştir. Bkz. Akbulut, Bilişim Alanında Suçlar, s. 196. Yine Akbulut' a göre silinen veriler yeni bir şey ifade ediyorsa, başka bir deyişle silinmeden olumlu bir sonuç çıkıyorsa bu verileri değiştirmek anlamında değerlendirilmelidir. Bkz. A.e., s. 198.
Yaşar-Gökcan-Artuç'a göre de: "Verinin bozulmasında ortada, bozulmuş da olsa bir veri vardır, bu veri kullanılamaz durumdadır, ancak bu veri onarılıp eski hale getirilebilir, oysa verinin yok edilmesinde ortada kullanılır veya kullanılamaz bir veri kalmamıştır, ortada bir veri yoktur, bu ikisi arasındaki fark da budur." Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7312.

gerekenin, verinin kayıtlı olduğu bellekten silinmesi suretiyle erişiminin mümkün olmaktan çıkarılması olduğu,[1092] bilişim alanında silmek ifadesinin de, esasen verilere ulaşımın engellenmesini, bazen kolayca bazen de uzun ve uğraştırıcı çalışmalar sonucu tekrar elde edilmesini ifade ettiği[1093] belirtilmektedir. Geri dönüşüm kutusuna gönderilen verilerin verileri yok etmek fiili kapsamında sayılıp sayılmayacağı ise doktrinde tartışmalı olup bir görüşe göre mantıki silme ile gerçekleşen bu hal, verinin mağdur açısından yok edilmiş olması anlamına gelmekte[1094] olup diğer görüşe göre ise ortadan kaldırılan veriye tekrar ulaşabilme imkânının varlığı suçun oluşumuna engel teşkil etmese de geri dönüşüm kutusuna atılan veriler bu kapsamda değerlendirilemeyecektir.[1095] Ayrıca doktrinde virüsler aracılığıyla bilişim sistemine zarar vermekle de verilerin yok edilebileceği ancak bu nitelikte bir fiilin sistemin işleyişinin engellenmesi veya bozulması kapsamında olmaması gerektiği belirtilmiştir.[1096]

3.2.2.2.3.2.3. Verileri Değiştirmek

Verilerin değiştirilmesi, verilerin orijinal halinden başka bir hale dönüştürülmesi,[1097] yeni içerik kazandırılması, niteliklerinin değiştirilmesi,[1098] verinin bulundurulma ve kullanma amacı dışında başka bir formata dönüştürülmesi,[1099] var olan verinin kullanımını engellemeyen ancak verinin kendisinin veya içeriğinin orijinalliğini ortadan kaldıran her türlü değişiklik,[1100] kaydedilmiş verinin başka bir bilgi içeriği almasını sağlayan her tür hareket[1101] olarak tanımlanmaktadır. Verilerin değiştirilmesi, içerik değiştirilmesinin her formu, içerik değiştirmeksizin başka bir program dili koduna çevirme, şifrenin değiştirilmesi,[1102] bir bilgi notu veya fotoğrafın değiştirilmesi, verilerden oluşan uygulama yazılımının değiştirilmesi şekillerinde

1092 Özbek, v.d., a.g.e., s. 939.
1093 Soyaslan, a.g.e., s. 646.
1094 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 324.
1095 Koca ve Üzülmez, a.g.e., s. 830; Yaşar, Gökcan ve Artuç, a.g.e., s. 7312.
1096 Akbulut, *Bilişim Alanında Suçlar*, s. 197.
1097 Parlar ve Hatipoğlu, a.g.e., s. 3751.
1098 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6933.
1099 Özbek, v.d., a..g.e., s. 939.
1100 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 140; Koca ve Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 830; Yaşar, Gökcan ve Artuç, a.g.e., s. 7312.
1101 Akbulut, *Bilişim Alanında Suçlar*, s. 197, 198.
1102 A.e.

gerçekleştirilebilir.[1103] Yine verinin tamamen veya kısmen değiştirilmesi arasında bir fark bulunmamaktadır.[1104]

3.2.2.2.3.2.4. Verileri Erişilmez Kılmak

Verilerin erişilmez kılınması, verilere erişimi sağlayan verilerin değiştirilmesi ve silinmesi suretiyle söz konusu verilere ulaşım imkânının ortadan kaldırılması,[1105] verilere erişmek için gerekli olan işlem bağının koparılması ile hak sahibinin olağan şekilde ve istediği zaman veriye ulaşımın engellenmesi,[1106] başka bir anlatımla verinin içerik bakımından bütünlüğünün korunmasıyla beraber verinin içerdiği bilgi veya enformasyona müdahale edilmeden veriye olağan şekilde erişimin engellenmesidir.[1107] Bu fiil verilerin bulunduğu bilişim sisteminin veya veri taşıma aracının bozulması, verilere ulaşılmak istendiği anda elektriğin kesilmesi şeklinde gerçekleştirilebileceği gerçekleştirilebileceği gibi verilerin başka bir yere taşınması, sisteme virüs bulaştırılması, şifre koyulması,[1108] güvenlik engellerinin veya şifrenin değiştirilmesi[1109] gibi çeşitli hareketlerle gerçekleştirilebilecektir. Kötü amaçlı yazılımlardan fidye yazılımlar ise bu fiili oluşturan en iyi örnektir.[1110] Bunun yanında Yargıtay kararlarına bakıldığında e-posta ve sosyal medya hesaplarının şifresinin değiştirilmesi suretiyle hesap sahibinin erişiminin engellenmesini 244. m.'nin 2. fıkrası kapsamında değerlendirdiği görülmektedir.[1111]

Doktrinde virüs saldırıları gibi hareketlerin bir bütün olarak bilişim sisteminin işleyişine yönelik bir saldırı niteliğinde olması halinde sistemin işleyişinin engellenmesi bazı durumlarda ise bozulması söz konusu olacağından bu hallerde

---

1103 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 324; Soyaslan, a.g.e., s. 646.
1104 Yaşar, Gökcan ve Artuç, a.g.e., s. 7312; Parlar ve Hatipoğlu, a.g.e., s. 3751.
Yargıtay 8. Ceza Dairesi' nin bir kararında:
"08.12.2010 tarihli Turkcell ve 01.06.2011 tarihli Telekom'un yazıları içerinden, 13.11.2009 tarihinde katılanın tarifesinde gerçekleştirilen online tarife değişikliğinin sanık adına kayıtlı IP adresi üzerinden gerçekleştirildiğinin anlaşılması karşısında sanığın TCK'nın 244/2. madde ve fıkrası uyarınca mahkumiyeti yerine yazılı gerekçe ile beraatine hükmedilmesi, Yasaya aykırı, …(BOZULMASINA)" hükmedilmiştir. Bkz. Yargıtay 8. Ceza Dairesi, 7.12.2017 t., E: 2017/21008, K: 13932, https://legalbank.net/arama, ET. 15 Temmuz 2020.
1105 Parlar ve Hatipoğlu, a.g.e., s. 3751; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6933.
1106 Ketizmen,(2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 140; Koca ve Üzülmez, a.g.e., s. 830; Yaşar, Gökcan ve Artuç, a.g.e., s. 7312, 7313; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 324; Soyaslan, a.g.e., s. 646.
1107 Özbek, v.d., a.g.e., s. 939.
1108 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 324, 325; Soyaslan, a.g.e., s. 646.
1109 Akbulut, *Bilişim Alanında Suçlar*, s. 200.
1110 Karagöz, a.g.e., s. 125.
1111 Bkz. Yargıtay 11. CD., 10.12.2012 T., E: 2010/9658, K: 2012/21340; Yargıtay 15. CD., 15.11.2016, E: 2016/3871, K: 2016/8608.

sistemde yer alan verilere erişilememesinin 244. m.'nin 1. fıkrası kapsamında olacağı belirtilmekte[1112] olup biz de bu görüşe katılmaktayız. Nitekim, daha önce de belirtmiş olduğumuz gibi her somut olayda failin kastı önem taşımakla birlikte beraber sistemin tamamına yönelmiş bir saldırıda failin kastının da sistem içerisinde yer alan verilere erişimin engellenmesinden ziyade sistemin bütününün işleyişinin engellenmesine yönelik olduğu kabul edilebilecek ve neticeten 244. m.'nin 1. fıkrasından cezalandırılması yoluna gidilebilecektir. Zira sorun fikri içtima kuralları uyarınca değerlendirildiğinde de burada daha ağır ceza niteliği taşıyan 1. fıkra hükümleri uygulanacaktır.

3.2.2.2.3.2.5. Sisteme Veri Yerleştirmek

Sistemdeki mevcut verilere dokunmadan ve herhangi bir zarar vermeden sistem üzerinde hak sahibi olan kişinin rızasına aykırı olarak sisteme yeni veri girilmesi, yerleştirilmesi, yüklenilmesi[1113] olarak ifade edilen bu hareketle mevcut verilere bir zarar verilmemekle beraber bu veriler zarar görme tehlikesi ile karşı karşıya kalmaktadır.[1114] Bunun yanında veri yerleştirme fiili, izinli veya izinsiz girilen sisteme doğrudan veri girişi yapılmak suretiyle, usb cihazı, CD gibi veri taşıma araçları ile sisteme aktarım şeklinde veya internet ortamından sisteme veri yerleştirmek suretiyle de gerçekleştirilebilmektedir.[1115]

3.2.2.2.3.2.6. Var Olan Verileri Başka Yere Göndermek

Doktrinde, bilişim sistemi içerisindeki verilerin başka bir bilişim sistemine veya veri taşıma cihazına aktarılması, kaydedilmesi, gönderilmesi, kopyalanması[1116]

1112 Özbek, v.d., a.g.e., s. 939.

1113 Koca ve Üzülmez, a.g.e., s. 830; Yaşar, Gökcan ve Artuç, a.g.e., s. 7313; Parlar ve Hatipoğlu, a.g.e., s. 3752; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6934; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 328; Soyaslan, a.g.e., s. 646.

1114 Yaşar, Gökcan ve Artuç, a.g.e., s. 7313; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6934.

Artuk-Gökçen-Yenidünya' ya göre: "Şayet sisteme yerleştirilen veriler, daha sonra oluşturulan bir belgenin içeriğini etkilemişse, fail ayrıca belgede sahtecilikten sorumlu tutulur (m.212)." bkz. A.e.

1115 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 328; Soyaslan, a.g.e., s. 647; Koca ve Üzülmez, a.g.e., s. 830, 831; Akbulut, *Bilişim Alanında Suçlar*, s. 202.

1116 Ketizmen, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, s. 140; Koca ve Üzülmez, a.g.e., s. 831; Parlar ve Hatipoğlu, a.g.e., s. 3752; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6934; Yaşar, Gökcan ve Artuç, a.g.e., s. 7313; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 328; Soyaslan, a.g.e., s. 647.

Akbulut verileri başka bir yere gönderme fiilini; "telekomünikasyon yolları üzerinden veya mevcut ağ içerisinde bir sistemdeki verilerin başka bir sisteme gönderilmesidir." şeklinde tanımlamıştır. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 202.

olarak tanımlanan bu hareketin muğlak olduğu, bir bilişim sisteminde gerçekleşecek her türlü işlem için mutlak suretle bir veri iletiminin gerçekleşeceği, bu madde düzenlemesinin sistem içerisindeki verinin başka bir yere gönderilmesi olarak düşünülebileceği belirtilmektedir.[1117] Kanaatimizce kanun koyucu, madde içerisinde yer alan söz konusu hareketi boşluk bırakmamak adına düzenlemişse[1118] de bu hareket açısından da "belirlilik ilkesi" nin zedelenebileceği bir durum ortaya çıkmıştır. Nitekim Yargıtay vermiş olduğu bir kararında[1119] bilişim sistemine girerek orada bulunan verileri alıp kendi kullandığı bilgisayara ve CD' ye aktarma şeklinde gerçekleşen eylemin bir bütün olarak 244. m.'nin 2. fıkrası kapsamında değerlendirmiştir. Başka yerden anlaşılması hususunda ise, verilerin bulunduğu bilişim sistemi dışına transfer edilmesi gerektiğini belirten yazarlar[1120] bulunduğu gibi verinin aynı sistem içerisinde fakat başka bir yere gönderilmesi durumunda da bu

1117 Özbek, v.d., a.g.e., s. 940.
Özbek, Kanbur, Doğan, Bacaksız ve Tepe' ye göre, bu hareketin düzenleniş şekli maddenin "ratio legis"ine hizmet etmekten uzaktır. Bkz. A.e.
1118 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 329.
1119 "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 dair 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,… (BOZULMASINA)" hükmetmiştir. Bkz. Yargıtay 8. Ceza Dairesi, 14.7.2014 t., E: 2013/3173, K: 2014/18506, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Bir başka Yargıtay kararında ise: "Katılan Şirketin sahibi olduğu web sitesi, müşterilerine ilan yapmaya kul- lanıcılarına da bu ilanları görmelerine imkan sağlayan dolayısı ile bu ilanlar üzerinden de karşılıklı iletişim sağlanarak alışveriş imkanı yaratan hizmet kolunda faaliyet gösterdiği ve kendisine verilen ilanlardan oluşan internet sitesi bazında bir veri tabanına sahip oldu- ğu, sanığın da bu şirkete ait web sitesindeki veri tabanınındaki ilanlara erişip izinsiz olarak kendisine ait internet sitesine gönderip kullanarak üzerine atılı bilişim sistemindeki verileri başka yere göndermek ve kullanmak suçunu işlediğinden bahisle açılan davada;
Sanık kurduğu sitenin arama motoru görevi gördüğünü, yaptığı işlerin link vermek şeklinde olduğunu savunmuştur. Katılan ise link verilmesi dahi izne tabi olup olayda sanık şirketin sayfasını kopyalayıp kendi sayfasına almış, ancak silemediği için logonun o sayfada görülmekte olduğunu belirterek şikayetçi olmuştur.
Bilirkişi, örümcek olarak tabir edilen bu sistemin çeşitli internet sitelerinde belirli kelime aramaları yaparak verileri çekmekte ve bu konuda arama motoru görevi yapmakta olduğunu, sitede ilanların hangi sayfadan alındığı görünmekte ve o siteye link verilmekte olup ilgilenen kişi gerçek bilgiye kendi sitesinde ulaşabildiğini bunların içerisinde katılan şirketin web sayfasında bulunan ilanların da bulunduğunun tespit edildiğini belirtmiştir.
İnternette ilanla mal satışlarında, ilanlar belirlenen süre ücretsiz olup daha sonraki ilanlar ücretli yayınlanabildiği dikkate alındığında ve dosya içinde bilirkişi rapo- runa ekli sayfa görüntülerinde; ilanda katılan şirketin logosu da dahil olmak üzere örneğin satılık arabanın resmi, teknik özellikleri, bedeli ve satıcı bilgileri tümüyle yayınlanıp alıcının tekrar katılan şirkete ait siteye gitmesine gerek kalmadığı açıkça görülmekte olup bilirkişi raporunda bahsolunan" çeşitli internet sitelerinde belirli kelime aramaları yaparak verileri çekmekte bu konuda arama motoru görevi yapmak"tan farklı olduğu anlaşılmakla, dosyaya uygun düşmeyen bilirkişi raporuna dayanarak ve eylemin TCK.nun 244/2. maddesindeki suçu oluşturup mahkumiyetine karar verilmesi gerektiği gözetilmeden, yazılı şekilde beraatine karar verilmesi, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 14.5.2014 t., E: 2013/4675, K: 2014/12406, https://legalbank.net/arama, ET. 15 Temmuz 2020.
1120 Koca ve Üzülmez, a.g.e., s. 831.

hareketin oluşacağını dolayısıyla mağdura ait olmayan başka bir bilişim sistemine gönderilmesinin şart olmadığını belirten yazarlar[1121] da bulunmaktadır.

Verileri başka bir yere göndermek aynı veri yerleştirmede olduğu gibi, veri iletim ağları üzerinden gerçekleştirilebileceği gibi, usb cihazı, CD gibi veri taşıma araçları üzerine kaydedilerek veya internet ortamında verinin aktarılması suretiyle de gerçekleştirilebilmektedir.[1122]

Burada değinilmesi gereken bir husus da verinin aslının mı kopyasının mı transferinin bu kapsamda olduğu başka bir deyişle verilerin kesilerek gönderilmesi ile kopyalanarak gönderilmesi arasında bir fark bulunup bulunmadığıdır. Doktrinde, madde kapsamında kastedilenin verinin yeni bir kopyasının başka bir sisteme aktarılması olduğu zira aslının gönderilmesi halinde verilerin yok edilmesinin oluşacağı bunun da madde kapsamında fakat ayrı bir hareket olduğu ifade edilmektedir.[1123]

3.2.2.3. Manevi Unsur

244. m.'nin 1. ve 2. fıkrasında düzenlenen suçların manevi unsurunu kast oluşturmakta olup bu suçların taksirle işlenmesi hali suç olarak düzenlenmediğinden taksirle işlenen hali suç oluşturmayacaktır.[1124] O halde, fail gerçekleştirdiği eylemi, sonuçlarını ve bu eylemi gerçekleştirirken sonucunda bir zararın meydana gelmesini de istemelidir.[1125] Bunun yanında, söz konusu suç tiplerinde kastın dışında başka bir manevi unsur aranmadığından bu suçlar olası kastla da işlenebilecektir.[1126]

1121 Yaşar, Gökcan ve Artuç, a.g.e., s. 7314; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6934.

1122 Parlar ve Hatipoğlu, a.g.e., s. 3752; Yaşar, Gökcan ve Artuç, a.g.e., s. 7313, 7314; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 329; Soyaslan, a.g.e., s. 648.

1123 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 328; Soyaslan, a.g.e., s. 647, 648. Yaşar,Gökcan ve Artuç' a göre de: "…burada kanaatimizce gönderilen verinin kopyalanarak gönderilmesi ile kesilerek gönderilmesi arasında fark bulunmamaktadır, korunmaya çalışılan verinin kendisidir, özellikle alan kimse açısından verinin kopyalanarak kendisine gelmiş olması ile, kesilerek gelmiş olması arasında fark bulunmamaktadır. Eğer kesilerek verinin başka bir yere gönderilmesi şartı aranır ise, bu seçimlik hareketi, veriyi yok etmek seçimlik hareketinden ayırmak mümkün olmayacaktır." Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7313.

1124 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 334; Akbulut, *Bilişim Alanında Suçlar*, s. 203.

1125 Soyaslan, a.g.e., s. 649.

1126 Koca ve Üzülmez, a.g.e., s. 831; Soyaslan, a.g.e., s. 649; Akbulut, *Bilişim Alanında Suçlar*, s. 204.

3.2.2.4. Hukuka Aykırılık

244. m.'nin 1. ve 2. fıkralarında yer alan suç tipleri için hukuka özel aykırılık hali düzenlenmemiştir. 1. fıkra açısından bilişim sisteminin sağlıklı ve kesintisiz çalışmasında hak sahibi olan, 2. fıkra kapsamında ise veriler üzerinde tasarruf yetkisi bulunan kişinin rızası hukuka uygunluk sebebi oluşturacaktır.[1127] Bu duruma örnek olarak, sistemin güvenliğinin test edilmesi için görevlendirilen kişinin bu çalışma esnasında sistemin işleyişini bozması veya engellemesi veya verileri bozması, değiştirmesi verilebilir.[1128] Yine Ceza Muhakemesi Kanunu' nun (CMK) 134. m.'si uyarınca hakim kararıyla sanığın bilgisayar kütüklerinde arama yapılması, buradaki verilerin kopyalanması, CMK 135. m. uyarınca şüpheli veya sanığın iletişiminin denetlenmesi kapsamında elektronik postalarının kopyalanması, 5651 sayılı Kanun uyarınca erişimin engellenmesi kararının icrası da görevin ifası hukuka uygunluk sebebiyle haksızlık teşkil etmeyecektir.[1129]

3.2.2.5. Suçun Nitelikli Halleri

3.2.2.5.1. Suçun Bir Banka veya Kredi Kurumuna ya da Bir Kamu Kurum veya Kuruluşuna Ait Bilişim Sistemi Üzerinde Gerçekleştirilmesi (TCK madde 244/3)

244. m.'nin 3. fıkrasında cezayı artıran nitelikli hal, 1. ve 2. fıkralarda düzenlenmiş olan fiillerin bir banka veya kredi kurumuna veya bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek cezanın yarı oranında artırılması olarak düzenlenmiştir.[1130] 3. fıkranın cezayı artırıcı nitelikli hal olarak kabul edilmesindeki temel amacın günümüzde bankalar veya kredi kurumlarının birçoğunun finansal hizmetleri idarenin de birçok kamu hizmetini bilişim sistemleri aracılığıyla yerine getirmesi, bu hizmetlere ilişkin kayıtların da sistemde depolanıp işlenmesinin daha ağır neticelere sebebiyet verebilecek nitelikte olması,[1131]

1127 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 335.
1128 Akbulut, *Bilişim Alanında Suçlar*, s. 204.
1129 Koca ve Üzülmez, a.g.e., s. 831; Akbulut, *Bilişim Alanında Suçlar*, s. 204.
1130 Yargıtay 8. Ceza Dairesi, bilişim sistemindeki verilerini değiştirmek suretiyle ders notlarını ve devamsızlık durumlarını değiştirdiklerinden bahisle sanıklar hakkında açılan bir davada: "Sanıkların okul ders notlarını ve devamsızlık durumlarını değiştirmek için bilişim sisteminin Milli Eğitim Bakanlığı'na bağlı okullarda kullanılan e-okul bilişim sistemi şifreleri ele geçirmek suretiyle yükletilen suçu işledikleri kabul edilmesi sebebiyle hükmolunan cezasının sitenin kamu kurumuna ait olması sebebiyle TCK.nun 244/3. maddesi gereğince cezaların arttırılması gerektiği gözetilmeden yazılı şekilde hükümler kurulması," sebebiyle ilk derece mahkemesi kararının bozulmasına hükmetmiştir. Bkz. Yargıtay 8. CD., 15.2.2017 t., E: 2016/3794, K: 2017/1405, https://legalbank.net/arama, ET. 15 Temmuz 2020.
1131 Özbek, v.d., a.g.e., s. 941.

bu kurumların bilişim sistemi aracılığıyla tüm topluma hizmet etmesi, yerine getirdiği kamu hizmetinin aksaması halinde de toplumu oluşturan tüm fertleri mağdur edecek olması,[1132] özetle bu sistemlerin tüm topluma hizmet etmesi sebebiyle bunların düzenli çalışmasında tüm toplumun menfaatinin bulunması[1133] hususları gösterilmektedir.

Nitelikli halin uygulanmasını sağlayan banka kavramı, 5411 sayılı Bankacılık Kanunu' nun 3. m.'sine göre, mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını ifade etmekte olup fırkada belirtilen kamu kurum veya kuruluşları ise merkezi idare, yerel yönetimler ve hizmet yerinden yönetim kuruluşları da dahil olmak üzere tüm idari kuruluşları ifade etmektedir.[1134]

Doktrinde 3. fıkrada düzenlenen nitelikli halin kabul edilmesinin yerinde bir düzenleme olduğu, zira bu kuruluşların bilişim sistemlerine gerçekleştirilecek müdahalelerde hizmet verdikleri kesimler ve toplumun büyük bir kısmı açısından büyük sorunların meydana geleceği,[1135] başka bir deyişle bu kuruluşların sistemlerinin işlemesinin engellenmesinden doğan zararların kişilere oranla çok daha büyük miktarlara ulaşabileceği[1136] belirtilmektedir. Bunun yanında, bir şirket ya da işletme açısından da sistemin işleyişinin engellenmesinin çok fazla önem taşıyabileceği maddedeki nitelikli hal ile sadece banka veya kredi kurumu ya da kamu kurum ve kuruluşlarıyla sınırlandırmamanın uygun olacağı, bilişim sistemlerinin veya verilerin ait olduğu kurum ve kuruluşların, şirketlerin veya sistemin işleyişinin engellenmesinin uzun süre devam edebilecek olması da göz önünde bulundurularak artırım miktarında alt ve üst sınır kabul edilmesinin ve bu aralıklar arasında artırım yapılmasında hakime takdir yetkisi verilmesinin uygun olacağını belirten yazarlar[1137] bulunduğu gibi madde düzenlemesine ek olarak kamu görevlisinin veya banka ve kredi kurumu görevlisinin bu sistemlere daha kolay müdahalede bulunabileceği göz önünde bulundurularak bu kişilerin suçu işlemesi halinin cezayı artıran nitelikli hal olarak düzenlenmesinin uygun olacağını belirten yazarlar[1138] da bulunmaktadır. Kanaatimizce, madde içerisinde toplumun büyük bir kısmını etkileyecek ve hatta zarar verebilecek bir halin dikkate alınarak nitelikli bir hal düzenlenmesi yerinde ise de siber terör başlığı altında

1132 Koca ve Üzülmez, a.g.e., s. 832; Yaşar, Gökcan ve Artuç, a.g.e., s. 7314.
1133 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 198.
1134 Akbulut, *Bilişim Alanında Suçlar*, s. 206, 207.
1135 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 334.
1136 Akbulut, *Bilişim Alanında Suçlar*, s. 206.
1137 Akbulut, *Bilişim Alanında Suçlar*, s. 205, 206.
1138 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 197; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 334.

da belirtmiş olduğumuz üzere ülkenin kritik altyapılarına yönelmiş saldırıların (veya maddede belirtilen fiillerin) ayrıca dikkate alınarak düzenleme yapılmasında fayda görülmektedir. Nitekim, kritik altyapı olarak belirlenen hizmetler sadece kamusal tarafta yürütülen bir hizmet niteliği taşımamaktadır. Bu bağlamda ilgili başlık altında da belirtmiş olduğumuz üzere bu m.'ye 244/A şeklinde bir madde eklenilmek suretiyle kritik altyapılara yönelik fiillerin kamu veya özel sektör ayrımı yapılmaksızın bir bütün olarak hizmetin korunması anlamında ayrıca düzenleme altına alınması gerektiğini değerlendirmekle birlikte var olan 3. fıkra düzenlemesine de bu kurumlarda çalışan görevlilerin sahip oldukları imkanların kolaylığından faydalanmak suretiyle işlenmesi halinin eklenmesi bunun yanında maddede düzenlenen cezai yaptırım hususunda ise alt ve üst sınır belirlenmesinin daha yerinde bir düzenleme olacağı fikrine katılmaktayız.

3.2.2.5.2. Suçun Terör Amacıyla ve Terör Örgütünün Faaliyeti Çerçevesinde İşlenmesi

3713 sayılı Terörle Mücadele Kanunu' nun 4. m.'si[1139] uyarınca 5237 sayılı TCK' nın "Bilişim Alanında Suçlar" bölümünde yer alan 243 ve 244. m.'lerindeki suçların TMK' nın 1. m.'sinde belirtilen terör amacıyla, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlenmesi halinde terör suçu sayılacağı belirtilmiş olup aynı Kanun' un 5. m.'sinde ise söz konusu suçların (3. ve 4. m.) terör amacıyla işlenmesi halinde ilgili kanunlara göre tayin edilecek hapis cezaları veya adli para cezalarının yarı oranında artırılarak hükmolunacağı, bu suretle tayin olunacak cezalarda o fiil için ve her nevi ceza için muayyen olan cezanın yukarı sınırının aşılabileceği ayrıca bu madde hükümlerinin çocuklar hakkında uygulanmayacağı belirtilmiştir.[1140]

1139 "Madde 4 –(Değişik: 29/6/2006-5532/3 md.)Aşağıdaki suçlar 1 inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır:a) Türk Ceza Kanununun 79, 80, 81, 82, 84, 86, 87, 96, 106, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 142, 148, 149, 151, 152, 170, 172, 173, 174, 185, 188, 199, 200, 202, 204, 210, 213, 214, 215, 223, 224, 243, 244, 265, 294, 300, 316, 317, 318 ve 319 uncu maddeleri ile 310 uncu maddesinin ikinci fıkrasında yer alan suçlar…" bkz. https://mevzuat.gov.tr/mevzuatmetin/1.5.3713.pdf, ET. 23 Mart 2010.

1140 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 274; Akbulut, *Bilişim Alanında Suçlar*, s. 208.

3.2.2.6. Kusurluluk

Söz konusu suç tipi kusurluluk açısından ayrı bir özellik arz etmemektedir.

3.2.2.7. TCK madde 244/1-2 ile İlgili Diğer Suçlar Arasındaki İlişki

TCK'nın 244. m.'sinin 2. fıkrasında yer alan suç ile kişisel verilere zarar verilmesi halinde TCK'nın 135- Kişisel verilerin kaydedilmesi ve 136- Verileri hukuka aykırı olarak verme veya ele geçirme suçları ile arasındaki ilişki gündeme gelecektir. Doktrinde, böyle bir durumunda varlığı halinde TCK 135 veya 136. m.'de yer alan suçun gerçekleşeceğini belirten yazarlar[1141] bulunduğu gibi somut olayın özelliklerine göre failin her iki suçtan sorumluluğuna gidilebileceği gibi 44. m. uyarınca sadece en ağır cezayı gerektiren suçtan cezalandırılabileceğini belirten yazarlar[1142] da bulunmaktadır. Yargıtay ise bir kararında[1143], banka ve kredi kartı bilgilerini kopyalamak için ATM' ye sistem kurma eyleminin 244. m.'nin 2. ve 3. fıkrasını değil 136. m.'de yer alan suçu oluşturduğuna, vermiş olduğu bir başka kararında[1144] ise katılanın cep telefonunu katılandan habersiz kendi kullandığı

1141 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 329.

1142 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345, s. 6936; Erdoğan, Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, s. 237; Mahmutoğlu, a.g.e., s. 870.
Akbulut' a göre de: "Türk Ceza Kanununun 244. maddesinde ifade edilen bilişim sisteminin işleyişinin engellenmesiyle haberleşmenin engellenmesi (TCK m. 124) de gerçekleştirilmiş olabilir. Tek fiille farklı suçların gerçekleştirilmesi söz konusu olduğundan fikri içtima kuralları uygulanmalıdır. Aynı şekilde m. 136 ile m. 244 arasında da fikri içtima söz konusu olabilir." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 212.

1143 "Bankanın ATM cihazına banka ve kredi kartları bilgilerini kopyalamak için sistem kuran, ancak ihbar edilmeleri neticesinde herhangi bir kartın kopyalamasını yapamadan yakalanan sanığın eyleminin TCK.nun 136, 35. maddelerine uyan suçu oluşturduğu gözetilmeden yazılı şekilde TCK.nun 244/2-3. maddeleri uyarınca hüküm kurulması,… BOZULMASINA" Yargıtay 8. Ceza Dairesi, 7.7.2014 tarihli, E: 2014/23, K: 2014/17639, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay 8. CD.' nin 21.1.2015 tarihli, E: 2014/30107, K: 2015/1395 sayılı kararında: "Sanıklar hakkında "bilişim sistemindeki verileri başka yere gön- derme" suçundan kurulan mahkumiyet hükümlerine yönelik temyize gelince;
Sanıkların ... girişine yerleştirdikleri düzenekle mağdurların kart bilgilerini ve şifrelerini elde etmekten ibaret eylemlerinin, katılan bankaların bilişim sistemlerine girilmemiş olması ve kredi kartının bilişim sistemi olmaması sebebiyle TCK. nun 244/2-3. madde fıkrasındaki suçun unsurlarının oluşmadığı gözetilmeden, bilişim sistemindeki verileri başka yere gönderme suçundan yazılı şekilde mahkümiyetlerine karar verilmesi, … (BOZULMASINA)" hükmedilmiştir. Bkz. https://legalbank.net/arama, ET. 15 Temmuz 2020.

1144 "Dosya kapsamına göre; sanığın, katılanın cep telefonunu katılandan habersiz kendi kullandığı bilgisayara bağlayarak içerisinde bulunan rehber ve media dosyalarının tamamını ele geçirdiği ve cep telefonundaki kayıtları sildiği iddia ve kabul edilen olayda, sanığın sübut bulan eylemleri nedeniyle TCK'nın 244/2. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme, aynı Kanunun 134/1 maddesinde düzenlenen özel hayatın gizliliğini ihlal ve 136/1 maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçlarını oluşturduğu gözetilmeden sadece TCK'nın 136/1. maddesinde düzenlen verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanığın mahkumiyete karar verilmesi…" Yargıtay 12. Ceza Dairesi,

bilgisayara bağlayarak içerisinde bulunan rehber ve media dosyalarının tamamını ele geçirme ve cep telefonundaki kayıtları silme eylemleri nedeniyle TCK' nın 244/2. m.'sinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme, 134/1 m.'sinde düzenlenen özel hayatın gizliliğini ihlal ve 136/1 m.'sinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçlarının oluştuğuna hükmetmiştir. Kanaatimizce de ikinci görüşte belirtildiği gibi somut olayın özelliklerine göre ve failin kastı da dikkate alınmak suretiyle ve aynı fiil ile gerçekleştirilip gerçekleştirilmemesi değerlendirilerek failin ilgili suçlardan gerçek içtima uyarınca sorumluluğuna gidilebileceği gibi fikri içtima hükümleri uyarınca sadece en ağır cezayı gerektiren suçtan da cezalandırılabilecektir.

Bilişim sistemine veri eklenmesi, verilerin değiştirilmesi gibi eylemlerin gerçekleştirilmesi ile bir belgenin düzenlenmesine esas teşkil ettiği hallerde doktrinde failin ayrıca belgede sahtecilik suçundan da cezalandırılması gerektiğini belirten yazarlar[1145] bulunduğu gibi fikri içtima kuralları gereğince en ağır cezayı gerektiren suçtan sorumlu tutulması gerektiğini belirten yazarların[1146] yanında her somut olayda durumun ayrı ayrı değerlendirilmesi gerektiğini belirten yazarlar[1147] da bulunmaktadır.

18.10.2017 t., E: 2016/10576, K: 2017/7642, https://www.hukukmedeniyeti.org/karar/2789451/, ET. 15 Temmuz 2020.
'Yargıtay 12. Ceza Dairesi' nin aynı yönde vermiş olduğu 19.1.2015 tarihli, E. 2014/18179, K. 2015/564 sayılı kararında da: '…sanığın, facebook adlı sosyal paylaşım sitesinde, "Irem .." profili ile katılanla iletişim kurarak, katılanın arkadaşlık listesine dahil olduktan sonra, katılan facebook hesabına giriş için kullandığı elektronik posta adresini ve şifresini, onun bilgisi ve rızası dışında ele geçirip, başka bir elektronik posta adresiyle değiştirerek, katılanın facebook hesabı üzerinden, katılan tarafından yazılıyormuş algısı dolduracak şekilde, katılanın arkadaşlarına cinsel içerikli mesajlar gönderdiği ve katılanın bilişim sistemindeki kendisine ait kısma erişimini engellediğinin iddia edildiği olayda, 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, TCK'nın 61/1. maddesinde yer alan ölçütler nazara alınarak, dosyaya yansıyan bilgi ve kanıtlar birlikte ve isabetle değerlendirilip, denetime olanak verecek ve somut gerekçeler de gösterilmek suretiyle, aynı Kanun'un 3/1. maddesi uyarınca işlenen fiilin ağırlığıyla orantılı olacak şekilde maddede öngörülen alt ve üst sınırlar arasında hakkaniyete uygun bir cezaya hükmolunması gerekirken, temel cezanın asgari hadden tayin edilmesi, 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, aleyhe temyiz bulunmadığından bozma sebebi sayılmamıştır.' (*Aktaran* Apaydın, "Bilişim Sistemine Girme Suçu", s. 293, dipnot. 222)
1145 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6936; Mahmutoğlu, a.g.e., s. 870.
1146 Akbulut, *Bilişim Alanında Suçlar*, s. 211.
1147 "Örneğin; sahte resmi belge kullanılarak bilişim sistemine giriş izninin sağlanması ve sonrasında 244 (2) kapsamında sonuç doğuracak davranışlarda bulunulması halinde, sahte belge ve verilere müdahale için TCK'nın 212 kapsamında iki ayrı suçtan (TCK 204 ve 244 (2)) ceza tayin olunmalıdır. Diğer bir deyişle biz sahte belgenin verilerin tahribatı için bir şekilde kullanılması halinde iki ayrı suçun oluştuğunu, verilerde tahribat yapılarak sahte belge düzenlenmesi halinde ise, bu durumda fikri içtima (TCK m.44) kuralının uygulanması gerektiğini kabul ediyoruz. Zira

Yargıtay ise sağlanması vaad edilen maddi menfaat karşılığında sanığın kendisi ve yakınları hakkındaki iki adet soruşturma dosyasını Cumhuriyet Savcılarının odalarından gizlice alıp ilgili Cumhuriyet Savcılarının şifrelerini kullanarak giriş yaptığı UYAP ortamında soruşturma dosyalarıyla ilgili olarak suç ve taraf silme, taraf ekleme işlemlerini gerçekleştirmiş olduğu bir olay hakkında vermiş olduğu bir kararda gerçek içtima kuralları uyarınca iki suçtan (205/1-son ve 244/2. m.' leri) da cezalandırmasına hükmetmiştir.[1148] Kanaatimizce böyle bir durumun varlığı halinde de somut olayın özellikleri dikkate alınarak gerçek içtimanın uygulanması gerektiğini düşünmekteyiz. Zira, bu tür eylemlerde verilere müdahale eylemleri araç olarak kullanılmak suretiyle sahte bir belge düzenlenme, değiştirilme vb. işlemler gerçekleştirilmektedir. Mevzuatımıza bakıldığında ise AKSS' nin 7. m.'sinde düzenlenen bilgisayarla bağlantılı sahtecilik suçunun karşılığının bulunmadığı görülmekte olup failin verilere müdahale eylemleri (244/2) ile farklı farklı suçları meydana getirmesi (205/1) söz konusu olduğundan ve esasen bu suçları tek bir fiil ile meydana getirmediğinden gerçek içtima kuralları uyarınca oluşan ilgili suçlardan ayrı ayrı cezalandırılması yerinde olacaktır. Ancak burada AKSS' nin ilgili m.'sinin mevzuatımızda düzenlenmesinin de isabetli olacağını düşündüğümüzü belirtmek isteriz. Bu bağlamda, bilişim sisteminde yer alan verilere müdahale suretiyle sahte bir belge oluşturulmasına esas olması hali belgede sahtecilik suçları açısından cezayı artırıcı nitelikli hal olarak kabul edilebilecektir.

244/1-2. m. ile 142/2-e m.' de yer alan bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık suçu arasındaki ilişki açısından ise Yargıtay kararlarının ise

---

TCK'nın 212'nci maddesinde özel içtima hali düzenlenirken açıkça "başka suçun işlenmesi sırasında kullanılması halinde" denilmiştir." Bkz. *Erdoğan, Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 237, 238.

1148 "Sanık U.. K..'ın azmettirmesi ile hareket eden T.. K..'nın iki ayrı soruşturma dosyasını adliyeden çıkarıp bu kişiye teslim etmesi yanında bu dosyalarla ilgili olarak UYAP ortamında gerçeğe aykırı işlemler yapması şeklindeki eylemlerinde, TCK'nın 142, 204, 281. maddelerinde düzenlenen suçların unsurlarının bulunmadığı, buna karşın bilişim sistemindeki verileri değiştirme suçunun işlenmesi için fiziki evrakın da yok edilmesi veya gizlenmesinin zorunlu olmaması nedeniyle hukuki anlamda tek bir fiilden söz edilemeyecek ve TCK'nın 44. maddesi uyarınca fikri içtima kuralının uygulanamayacak olması karşısında, sanıkların unsurları oluşan resmi belgeyi gizleme ve bilişim sistemindeki verileri değiştirme suçları dolayısıyla TCK'nın 205/1-son ve 244/2. maddeleri uyarınca ayrı ayrı cezalandırılmaları gerektiği ve anılan suçları oluşturan eylemlerin aynı zaman diliminde aynı suçun işlenmesine matuf kesintisiz birer fiil olarak gerçekleştirilmiş olmaları sebebiyle anılan Yasanın 43/1. maddesinde düzenlenen zincirleme suç hükümlerinin uygulanma imkanının da bulunmadığı, gizlenen resmi belge adedi ile UYAP ortamında yapılan işlem sayısının ancak sübuta eren suçlar dolayısıyla verilecek temel cezaların belirlenmesinde dikkate alınabileceği gözetilmeden sadece resmi belgeyi gizleme ve bu fiile azmettirme suçlarından yazılı şekilde mahkumiyet hükümleri kurulması,…" bkz. Yargıtay 5. CD., 3.7.2014, E: 2014/ 6872, K: 2014/7366, https://www.hukukmedeniyeti.org/karar/2161414/yargitay-5-ceza-dairesi-e-2014-6872-k-2014-7366/, ET. 15 Temmuz 2020.

somut olayda sanığın kastı dikkate alınarak bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık suçunun oluştuğu yönünde olduğunu söyleyebilmekteyiz.[1149]

Son olarak 244/1-2. m. ile dolandırıcılık suçu arasındaki ilişki bakımından ise, e-mail adresi ve Facebook profilinin şifresinin ele geçirilerek değiştirilmek suretiyle internet ortamından 100 kontör gönderilmesinin istenildiği, gönderilmediği takdirde maddi zarara uğratılacağının bildirilmesi üzerine şikayetçi tarafından da kontörün gönderilmesi üzerine açılan bir davada Yargıtay, e-mail şifresinin ele geçirilmesi ve değiştirilmesi eyleminin TCK' nın 244/2. m.'sini, kontör talebinde bulunulmasının ise dolandırıcılık suçunu oluşturacağından bahisle hüküm kurulması gerektiğine hükmetmiştir.[1150]

1149 "Katılanın bilgisi ve rızası olmaksızın şifre bilgilerini ele geçirerek "www.....com" isimli internet sitesinden 12.02.2011 ve 14.02.2011 tarih- lerinde 100, 200, 200, 200, 50, 50 TL tutarlı 6 ayrı işlemle toplam 800 TL tutarlı kontör alımı gerçekleştirerek dolandırıcılık ve bilişim sistemine girme suçlarını işlediğinden bahisle açılan davada, sanığın atılı suçlamayı kabul etmeyip kontör yüklemede kullanıl- dığı belirtilen cep telefon numarasının kendisine ait olmayıp S. A. tarafından kullanıldığını, kendisinin sadece mesajlaşmak için o gün kullandığını, tanığın beyanını bu yönden kabul etmediğini savunması, tanık E. Y.'ın 07.03.2011 tarihinde işlenen başka suçla ilgili olarak alınan ve telefon numarasını sanığın kullandığına dair beyanı, cep telefon numarasının başkasına ait olup bu kişinin de resmi dışındakileri kabul etmemesi nedeniyle hakkında takipsizlik kararı verilmesi, kontör yüklenen telefon numaralarını kullanan hat sahiplerinin belirlendiği, ancak dinlenmediklerinin anlaşılması karşısında; GSM operatöründen abone belgelerinin asıllarının getirtilip yazı, rakam ve imza yönünden üzerinde inceleme yaptırılması, suç tarihleri itibariyle cep telefon numarasının kullanıldığı, cihazın İMEİ numarasının tespiti ile kime ait olduğunun araştırılması, kontör yüklemesi yapılan hat sahiplerinin dinlenerek sanıkla bağlantısı olup olmadığının belirlenmesi, eylemin bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturup oluşturmayacağı da tartışılarak sonucuna göre sanığın hukuki duru- munun tayin ve takdiri gerekirken, eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 26.10.2015 t., E: 2015/3118, K: 2015/23401, https://www.lexpera.com.tr/, ET. 15 Temmuz 2020.
"Yargıtay Ceza Genel Kurulu'nun 17.11.2009 gün ve 193/268 sayılı kararında açıklandığı üzere; sanığın, bir şekilde haksız olarak ele geçirdiği katılanlara ait bankacılık bilgilerini kullanarak internet aracılığıyla, katılanların..... Bankası nezdinde bulunan banka hesaplarından, aynı bankanın ..... Şubesi nezdinde bulunan kendi hesabına para havale edip çektiğinin anlaşılması karşısında; sanığın kastının katılanların banka hesabında bulunan parayı bilişim sistemini kullanmak suretiyle kendisinin kullanımındaki banka hesabına geçirmeye, katılanların rızasına aykırı olarak mal varlığında azalmaya neden olmaya, başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil edildiği parayı alarak mal edinmeye yönelik olduğu, eyleminin 5237 sayılı TCK.nun 142/2-e maddesine uyan hırsızlık suçunu oluşturduğu gözetilmeksizin yazılı şekilde anılan yasanın 244. maddesinden hüküm kurulması, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 29.2.2016 t., E: 2015/8512, K: 2016/ 2308, https://legalbank.net/arama, ET. 15 Temmuz 2020.
"…İnternet üzerinden müştekilerin yetkilisi oldukları şirket banka hesaplarından bilgi ve rızaları dışında suç tarihlerinde sanıklara ait ve belirledikleri hesaplara paraların aktarılması, çekilmesi veya bu hesaplardan alışveriş yapılması eyleminin TCK'nın 142/2-e. maddesindeki suçu oluşturduğu gözetilmeyerek yazılı şekilde TCK'nın 244. maddesi uyarınca hüküm kurulması,… BOZULMASINA" bkz. Yargıtay 13. Ceza Dairesi, 15.6.2017 t., E: 2017/2912, K: 2017/7281, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Aynı yönde bkz. Yargıtay 6. Ceza Dairesi, 19.6.2014 t., E: 2013/35219, K: 2014/12749; Yargıtay 13. Ceza Dairesi, 22.1.2015 t., E: 2014/18555, K: 2015/1618.
1150 "Şikayetçiye ait e-mail adresi ve Facebook profilini haksız olarak şifre- sinin ele geçirilip değiştirildiği, daha sonra internet ortamında 100 kontör göndermesi istendiği, kontör göndermediği takdirde her şeyin elinde olduğunu, ekran kartını yakaca- ğını, maddi hasara uğratacağını bildirmesi

3.2.2.8. TCK madde 243 ile 244/1-2 ile İlgili Diğer Suçlar Arasındaki İlişki

TCK' nın 243. m.'si ile 244/1-2. m.'leri arasındaki ilişki bakımından doktrinde farklı görüşler bulunmaktadır. Bir görüşe göre, 243. m.' de yer alan bilişim sistemin hukuka aykırı olarak girme veya sistemde kalma suçu 244. m. açısından geçit suçu oluşturmakta olup bu durumda fail sadece 244. m.' nin 1. veya 2. fıkrasından cezalandırılacaktır.[1151] Bir başka görüşe göre ise, 243. m. ile 244. m.' de düzenlenen

üzerine şikayetçinin 100 kontör gönderdi- ğinden bahisle açılan davada; suça sürüklenen çocuğun suçlamayı kabul etmeyip, kendine ait e-mail adresinin de arasıra çalınıp geri iade edildiğini, şikayetçiyi tanımadığını savun- ması, şikayetçinin Cumhuriyet Savcısına verdiği ifadesinde,...._@hotmail.com adıyla elektronik posta adresi ve bu adrese bağlı MSN kaydı bulunmakta olup bu mail adresine başka bir hotmail.com adresinden dosya gönderildiğini gelen dosyayı açar açmaz virüs uyarısı geldiğini, MSN'den Hicran isimli arkadaşıyla konuştuğunu düşünerek yazıştığını, bu dosya transferinin de MSN'de yazışırken gerçekleştiğini, gönderilenin okey oyunu hilesi olduğunu söylendiği, bu olayın Ocak ayının 8-9'unda akşam saat 20.00 sıralarında evinde gerçekleştiğini, virüslü dosya gelince arkadaş listesine eklediği Hicranı ve gelen dosyayı bilgisayarından sildiğini, 11.01.2012 tarihinde saat 19.00 sıralarında www.facebook.com isimli siteye s.....@windowslive.com adlı posta adresi aracılığında S.. Ö.. adlı kullanıcıya bağlanmak istediğinde önce girdiğini, ancak kendiliğinden çıkış yaptığını, hareket ettirmeden mause çubuğunun oynamaya başladığını, tekrar Facebooka bağlanmak istediğinde bağlanamadığını, Facebook kullanıcı adı ve şifresinin çalındığını anladığını, annesinin Facebook'undan girdiğinde kendi profilinin online olduğunu görüp, yazdığını, karşıdaki kişinin MSN'den yazışmak istemesi üzerine s.o...@windowslive.com adlı posta adresi aracılığında MSN'de bağlanıp yazıştığında karşısına c..a.@hotmail.com kullanıcısı çıktığı ve sunduğu yazışmayı yaptıklarını, kontör istemesi üzerine İslam adlı arkadaşı aracılığıyla kontör alıp şifreyi verdiğini, onun da Facebook hesabını geri verdiğini belirttiği, ayrıca mahkemede, yazıştığı kişinin bil- gisayar konusuna hakim birisi olduğunu, sanığın bu kişi ile aynı olduğunu düşünmediğini belirtmesi, Microsoft şirketinden gelen cevapta suç tarihinde şikayetçinin e-mail adresine giriş yapanların kendisi ve İ. K. kişi olduğunun bildirildiği, bunun dışında başka girişin tespit edilemediği gibi suça sürüklenen çocuğun el konulan bilgisayar içindeki harddisklerde yapılan bilirkişi incelemesi sonucu alınan raporda, çalındığı belirtilen e-mail adresi ve Facebook hesabına ilişkin kayıtlar olmadığı sadece şikayetçinin sonradan bağlantı kurmak üzere kullandığı s.ozger@windowslive.com adlı posta adresi ile yazışmalar olduğunun saptanması, kontör yüklenen telefon numarasının da başka bir kişinin kullanımında bulunması nedeniyle bu kişi hakkında suç duyurusunda bulunulması, bu telefon hattını arayanlar arasında suça sürüklenen çocuğun amcasının bulunduğunun iletişim kayıtlarından belirlenmesi, telefon hattının ise kayıtlarda S. Ç. adlı kişi adına kayıtlı olduğunun anlaşılması karşısında, kontör yüklenen telefon hattı ile ilgili belgelerin istenmesi ve bu kişinin tanık sıfatıyla dinlenmesi, suç duyurusu üzerine yapılan işlemlerin sorulması ve sonucunun araştırılması, ayrıca şikayetçinin e-mail adresine gir- diği anlaşılan İslam Karakoyun'un da bilgisine başvurulması, ayrıca e-mail şifresinin ele geçirilmesi ve değiştirilmesi eyleminin TCK.nun 244/2. maddesi kapsamındaki suçu, kontör talebinde bulunulmasının ise dolandırıcılık suçunu oluşturacağı da dikkate alınarak sonucuna göre tüm deliller yeniden değerlendirilip hukuki durumun tayin ve takdiri gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 18.11.2015 t., E:2015/11682, K: 2015/24706, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1151 "Gerçekten de bir çok olayda bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi eylemlerinin gerçekleştirilmesi için öncelikle bilişim sistemine hukuka aykırı olarak girilmesi ve orada hukuka aykırı olarak kalınması gerekmektedir." Bkz. Soyaslan, a.g.e., s. 650.

Artuk,Gökçen ve Yenidünya' ya göre de: "Bilişim sistemine hukuka aykırı erişim ve sistemde kalmaya devam etme, bilişim sistemlerine girerek işlenmesi zorunlu bulunan başka bilişim suçlarının işlenmesi için bir araçtır. Bu itibarla 243'üncü maddede yer alan suç, daha sonra işlenen bu suçlar bakımından bir geçit olma özelliği taşır ve fail sadece amaç suçtan dolayı cezalandırılır." Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345, s. 6912,* 6913.

Yazıcıoğlu ise 243. madde ile 244. madde arasında cezalandırmanın hangi maddeye ilişkin olacağı hususunda: "…, 244üncü maddedeki suçlar (sistemin donanımsal yanına zarar verme fiilleri hariç)

suçlar arasında fikri içtima hükümleri uygulanmalıdır.[1152] Bir diğer görüşe göre ise hangi suçun oluştuğu hususunda failin kastı dikkate alınarak çözüme ulaşılmalıdır.[1153] Dülger' e göre ise 243. m. ile 244. m. bu açıdan incelendiğinde bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçundaki her hareket için ve her somut olayda, mutlaka sisteme girme ve orada kalmaya devam etme suçunun işlenmesi gerekmemekte, bu nedenle her somut olay ve hareket açısından geçit suçuna ilişkin bu şekilde değerlendirme yapılarak verileri yerleştirme ve başka yere gönderme hareketlerinin öncesinde sisteme girilmeden gerçekleştirilmesi olanaklı olmadığından hukuka aykırı olarak girme suçunun bu

---

hukuka aykırı girme ve orada kalmaya devam etme fiilleri gerçekleşmeden işlenemezler; kanaatimizce, 244 üncü maddedeki fiiller zorunlu olarak 243/1 deki suçu içermektedir ve Kanunkoyucu açıkça göstermese de 243/1 inci maddedeki suç, 244 üncü maddedeki fiillerin unsuru teşkil etmektedir(md.42/1). Diğer taraftan her ne kadar TCK.da açık bir hüküm yoksa da geçitli suç hükümlerinin uygulanması suretiyle iki suçtan değil yani hem 243 üncü maddedeki suçtan hem de gerçekleştirilen final suçtan değil, sadece final suçtan cezalandırmanın yapılması gerektiğini düşünmekteyiz." Bkz. Yılmaz Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", s. 1260.

Dülger' e göre ise: "…Bu bağlamda bana göre eylemler arasında zamansal açıdan yakınlık bulunması halinde 244/2'den ceza verilmesi, zamansal açıdan yakınlık olmayıp farklı kastlarla hareket edildiğinin kabul edilmesi halinde ise her iki suçtan ayrı ayrı ceza verilmesi gerekir.

…geçit suçu, bir suçun işlenmesi için öncelikle cezası daha hafif olan bir suçun işlenmesi, bu suçtan geçilmesinden gerekmesi halidir. Ancak geçit suçunun söz konusu olabilmesi için işlenen ilk suçun ve sonraki daha ağır suçun aynı hukuksal değeri koruması gerekir. Oysa 243. maddede bilişim sisteminin güvenliğini korumakta iken yukarıda bahsetmiş olduğumuz suçlarda 244. madde hariç farklı hukuksal değerler de korunmaktadır. Bu nedenle her somut olay ve hareket açısından değerlendirme yapılması gerekir…243. madde ile 244. madde bu açıdan incelendiğinde bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçundaki her hareket için ve her somut olayda, mutlaka sisteme girme ve orada kalmaya devam etme suçunun işlenmesi gerekmez…" bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 299, 300.

Aynı yönde bkz. Parlar ve Hatipoğlu, a.g.e., s. 3753; Doğan, a.g.e., s. 98; Gül, a.g.e., s. 92.

1152 Bkz. Koca ve Üzülmez, a.g.e., s. 833; Akbulut, *Bilişim Alanında Suçlar*, s. 211.

"Bir bilişim sistemindeki verileri değiştirmek isteyen fail, bu suçun icra hareketlerini gerçekleştirirken sisteme de girmekte ve dolayısıyla 243. maddeyi de ihlal etmektedir. Bu itibarla failin bu suçlardan yalnızca en ağır cezayı gerektiren 244. maddedeki suçtan dolayı cezalandırılması gerekir." Bkz. Koca ve Üzülmez, a.g.e., s. 833.

1153 Bu görüşü savunan Özbek, v.d.' ne göre "TCK m.244'te yer alan suçun işlenebilmesi için kural olarak bilişim sistemine girmek ve orada kalmak gerekir. Bu yönüyle iki hüküm arasında bir "geçitli suç" ilişkisinin bulunduğu söylenebilir…Ancak hemen ifade edelim ki biz geçitli suç kurumunu kabul etmiyoruz…

Aslında bu konudaki sorunu çözümlemek ve daha yalın bir yasal düzenleme yapmak bakımından m.243 ve 244 tek bir maddede birleştirilmeli m.243/1 suçun temel şekli olarak düzenlenerek diğer haller suçun nitelikli haline dönüştürülmelidir." Bkz. Özbek, v.d., a.g.e., s. 929.

"Bilişim sistemine girilip kalınarak sistemin bozulması halinde TCK m. 244 f. 1'in söz konusu olacağı, ayrıca TCK m. 243'ten ceza verilmeyeceği söylenebileceği gibi ikisinin birlikte gerçekleştiği durumlarda, failin kastı her iki eyleme de yönelikse her iki suçtan da ceza verileceği söylenebilir…kanaatimizce 243. madde, 244. madde açısından geçit suç olarak kabul edilemez. Zira, kalma eylemi, mütemadi özelliği gereği başta hukuka uygunken sonradan hukuka aykırı hale gelebilirken; girme eyleminin hukuka uygun gerçekleştiği durumlarda geriye dönük olarak hukuka aykırı hale geldiği kabul edilemez. Sisteme hukuka uygun bir şekilde girildiği durumlarda da 244. maddenin 1. fıkrası ihlal edilebileceğinden, 243. maddenin geçit suç olma özelliğinden bahsedilemeyecektir." Bkz. Yazıcı, "Ulusal Mevzuat ve Yargıtay İçtihatları Işığında Türk Ceza Kanunu'ndaki "Bilişim Alanında Suçlar"", s. 920.

hareketler bakımından cezalandırılmayan önceki hareketler olarak bul edilmesi ve failin sadece 244/2'den cezalandırılması, sisteme girilmeden gerçekleştirilmesi olanaklı eylemler için ise aralarında zamansal açıdan yakınlık bulunması halinde 244/2'den ceza verilmesi, zamansal açıdan yakınlık olmayıp farklı kastlarla hareket edildiğinin kabul edilmesi halinde ise her iki suçtan ayrı ayrı ceza verilmesi gerekir.[1154] Mahmutoğlu' na göre de bilişim sistemine girmeden de verilerin bozulması söz konusu olabilecek olup bilişim sistemine girme suretiyle 244. m.' nin 1. ve 2. fıkrasındaki suçların oluşması halinde tüketen-tüketilen norm ilişkisi gereği TCK 244' ün uygulanması gerekecektir.[1155] Yargıtay ise sisteme hukuka aykırı giriş yapılması suretiyle verilere müdahale halinde başka bir deyişle TCK 234/1 ve TCK 244/2'nin birlikte oluştuğu durumlarda TCK 244/2' den cezalandırma yoluna gitmekte[1156]

1154 Bkz. Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 299, 300.
"… 243. madde ile 244. madde bu açıdan incelendiğinde bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçundaki her hareket için ve her somut olayda, mutlaka sisteme girme ve orada kalmaya devam etme suçunun işlenmesi gerekmez. Zira sunucunun ya da bilgisayarın çekiçle tahrip edilmesi ya da sabit diskin hava ya da suyla temas ettirilmesi halinde de bu suç gerçekleşmiş olur. Dolayısıyla 243. madde ile diğer bilişim suçları arasında geçit suçu ilişkisi bulunup bulunmadığı her somut olayda ayrı ayrı değerlendirilmelidir." Bkz. A.e., s. 300.
1155 Mahmutoğlu, a.g.e., s. 869.
1156 Yargıtay 8. Ceza Dairesi, 18.2.2016 tarihli bir kararında "Mağdura ait elektronik postaya bağlı Facebook hesabının şifresini ele geçirerek bu adrese giren, yazışmalar yapan ve şifreyi değiştirmek suretiyle mağdurun anılan hesaba erişimin engelleyen sanığın eyleminin, TCK'nun 244/2. maddesinde düzenlenen suçu oluşturacağı gözetilmeden eksik ceza tayini, … (BOZULMASINA)" şeklinde karar vermiştir. Bkz. Yargıtay 8. Ceza Dairesi, 18.2.2016 t., E: 2015/9713, K: 2016/1868, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yargıtay 8. Ceza Dairesi: "Sanığın, şikayetçinin elektronik posta adresinin şifresini ele geçirip sistede kalmaya devam edip şifreyi değiştirerek erişimini engellendiğinden bahisle açılan davada, sanığın şikayetçinin E-Mail hesabına giriş yaptığının tespit edildiği, bu haliyle eylemin TCK.nun 243/1. maddesi kapsamındaki suçu oluşturacağı, ancak şikayetçi girişinin şikayet tarihinden bir ay öncesinden beri engellediğini iddia etmişse de buna ilişkin bir tespite rastlanmadığının anlaşılması karşısında; girişiminin engellendiğini belirttiği tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, şikayetçi tarafın- dan kendi adresine erişim sağlanıp sağlanmadığı tespit olunmamıştır. Sanık tarafından giriş yapılarak adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığının ilgili internet sağlayıcısından sorulmadığı anlaşılmıştır.
Bu itibarla yukarıda açıklanan yöntem izlenerek eksiklikler yerine getirilip gerektiğinde bilirkişiden de görüş alınarak sonucuna göre sübutun varlığı halinde eylemin TCK.nun 244/2 maddesindeki suçu oluşturup oluşturmayacağı da değerledirilip sanığın hukuki durumunun takdir ve tayini gerekirken eksik araştırmaya dayanarak ve oluşa uygun olmayan şekilde TCK.nun 243/1 ve 244/1. maddeleri gereğince hükümler kurul- ması suretiyle fazla ceza tayini, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 1.4.2015 t., E: 2015/2112, K: 2015/15394, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay 8. Ceza Dairesi'nin aynı yönde vermiş olduğu bir başka kararında: "…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, … (BOZULMASINA)" bkz. Yine Yargıtay 8. Ceza Dairesi, 14.7.2014 t., E. 2013/3173, K. 2014/18506, https://legalbank.net/arama, ET. 15 Temmuz 2020.

bilişim sistemine hukuka aykırı olarak girişin gerçekleştirildiği fakat verilere müdahalenin söz konusu olmadığı veya tespit edilemediği hallerde ise TCK 243.' den cezalandırma yoluna gitmektedir.[1157]

Kanaatimizce, bilişim alanında işlenen suçların teknik yapısı, somut olayın özelliklerini ayrıca dikkate alınmasını gerektirmektedir. Nitekim, ilgili başlıklar altında 244. m.' nin 1. fıkrası ile 2. fıkrasında yer alan suçların muhakkak bilişim sisteminin soyut unsurlarına yönelik gerçekleşmeyeceği bunun yanında fiziki müdahalelerin de bu suçu gerçekleştirebileceğini belirtmiştik. Dolayısıyla, sisteme girilmeksizin 244. m.' nin 1. veya 2. fıkrasındaki suçlar gerçekleştirilmiş ise burada geçit suçunun varlığından bahsedilemeyecek ancak sisteme girilmek suretiyle ve failin amacının sonraki daha ağır suça (1. veya 2. fıkrada yer alan suçlara) yönelmesi halinde geçit suçunun varlığı kabul edilerek sadece sonraki eylemden cezalandırılma yoluna gidilebilecektir.[1158] Bunun yanında, 243. m. ve 244. m.' nin 1. ve 2. fıkralarında yer alan suçlar arasındaki ilişki için fikri içtima hükümlerinin uygulanmasını uygun bulmamaktayız. Zira 243. m.' de yer alan bilişim sistemine girme veya orada kalma fiili ile 244. m.' nin 1. ve 2. fıkralarında yer alan fiiller tek fiil kapsamında değerlendirilemeyecektir.[1159] Doktrinde konu üzerindeki sorunun çözümü ve daha yalın bir yasal düzenleme yapılması bakımından 243. ve 244. m.' lerin bir m.' de birleştirilmesi, 243. m.' nin suçun temel şekli olarak düzenlenerek diğer hallerin suçun

---

Aynı yönde bkz. Yargıtay 8. Ceza Dairesi, 12.4.2016 t., E: 2015/14287, K: 2016/4903.

1157 "…1- Katılana ait .....@hotmail.com internet adresinin ve facebook hesabının sanık tarafından şifreleri kırılmak suretiyle girilerek kullanılamaz hale getirildiği iddia- sıyla açılan davada, katılanın E-Mail hesabına sanık tarafından giriş yapıldığının tespit edildiği ancak, girişinin engellediğini iddia edilmişse de buna ilişkin bir tespite rastlan- madığı ve ayrıca bu adresin faal olup olmadığı, katılan tarafından kendi adresine erişim sağlanıp sağlanmadığı da tespit olunmadığından, katılana ait e-mail adresinin şifresinin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığının ilgili internet sağlayıcısından ve e-mail adresinin bağlı olduğu şirketten sorulması, katılana ait bilgisayarının soruşturma aşmasında teslim alındığı, ancak bir incelemeye rastlanmadığının anlaşılması karşısında, anılan bilgisayarın uzman bilirkişi tarafından mesajlaşma kayıtları ile log kayıtlarını da içerir şekilde incelenip sonucuna göre, erişilmez kılındığı takdirde TCK.nun 244/2., aksi takdirde aynı yasanın 243/1. maddesi kapsamındaki suçları oluşturacağı dikkate alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 18.11.2015 t., E: 2015/7531, K: 2015/ 24704, https://legalbank.net/arama, ET. 15 Temmuz 2020.

"Şikayetçinin rızası olmadan e-mail ve Facebook hesabına girip şifrelerini değiştirmek suretiyle bilişim sistemine girmesini engellediğinden bahisle açılan davada; katılanın hesabına sanığın giriş yaptığının tespit edildiği, dosya içerisinde şifrelerinin değiştirilmesine dair bir tespitin bulunmadığı ve katılanın hesabının kullanılarak kontör istenen arkadaşları olduğu anlaşılmakla, kalmaya devam ettiğine ilişkin deliller de mevcut olduğundan, sanığın eyleminin TCK.nun 243/1. maddesi kapsamındaki suçu oluşturacağı gözetilmeden suç vasfında yanılgı sonucu yazılı şekilde hüküm kurulması, … (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 6.12.2017 t., E: 2017/7826, K: 2017/13823, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1158 Aynı yönde bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 298.

1159 A.e.

nitelikli haline dönüştürülmesi fikri ileri sürülmüştür.[1160] 243. m. incelenirken de belirtmiş olduğumuz üzere kanaatimizce de 243. ve 244. m.' lerin tek bir madde içerisinde toplanarak farklı fıkralar altında düzenlenmesi bilişim alanında suçların koruduğu hukuksal yararın ortak olması anlamında doğru bir bakış açısı oluşturacaktır. Zira, biz bir suçun işlenmesinde sadece bilişim sistemlerinin araç olarak kullanılmasının o suçun "bilişim suçu" olarak kabulü anlamına gelmediğini kabul ederek "bilişim alanında suçlar" başlığı altında düzenlenecek suçların bu alana ve kendilerine özgü nitelikleri bulunan ayrı suç tipleri olduğunu kabul etmekteyiz. Bu anlamda oluşabilecek durumlar failin kastına göre aşamalı olarak ancak tek bir madde içerisinde düzenlenmesinin hem sistematik açıdan daha doğru hem de uygulamada ortaya çıkan fikir ayrılıklarını da sona erdirebilecek olacağını düşünmekteyiz.

3.2.2.9. Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suretiyle Haksız Yarar Sağlama Suçu (TCK madde 244/4)

TCK' nın 244. m.' sinin 4. fıkrasında: *"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 beşbin güne kadar adlî para cezasına hükmolunur."* şeklinde düzenlenen hükmün bağımsız bir suç oluşturup oluşturmadığı hususunda doktrinde fikir ayrılıkları bulunmaktadır. Doktrinde yer alan bir görüşe göre bu düzenleme bağımsız bir suç düzenlemesi niteliğindedir.[1161] 4. fıkra düzenlemesinin bağımsız bir suç olduğunu kabul eden yazarlardan bazıları ise bu suçun oluşabilmesi için failin öncelikle 244. m.' nin 1. ve 2. fıkralarındaki suçları işlemesi daha sonra nedensellik bağı içerisinde kendisine haksız çıkar sağlaması gerektiği için bu suçun yapısı itibariyle bileşik suç

1160 Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1426; Özbek, v.d., a.g.e., s. 929.

1161 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6937; Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, s. 221; Mahmutoğlu, a.g.e., s. 241; Soyaslan, a.g.e., s. 651; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 339.

Eker' e göre de: "Bu fıkra ile 244. maddenin ilk fıkrasında belirtilmiş bulunan eylemlerin, Ceza Kanunu'nun çeşitli maddelerinde yer alan bazı geleneksel suç biçimleriyle karşılanamayacak olması halinde boşluk yaratmamak adına veyahut söz konusu eylemler hakkında geleneksel hükümlerin tipiklik/ modalite unsuru açısından uygulanmasında tereddüde mahal verilmemesi amacıyla ayrıca bir düzenleme yapılarak bağımsız norm teşkili sağlanmaya çalışılmıştır." Bkz. Eker, a.g.e., s. 127.

Doğan' a göre de: "…kanun koyucunun dördüncü fıkrada bir suçta bulunması gereken tüm unsurlara yer verip, eylemin aynı zamanda başka bir suç oluşturması halinde hangisinin uygulanacağına dair eşitler arası bir değerlendirme yapması ve fıkrada artırım oranını belirlemek yerine doğrudan ceza belirlemiş olması hususları birlikte değerlendirildiğinde fıkrayı ayrı bir suç olarak düzenlemek istediği sonucu ortaya çıkmaktadır. Yargıtay da bir çok kararında bu suçun bağımsız bir suç olduğunu kabul etmiştir." Bkz. Doğan, a.g.e., s. 144.

olduğunu belirtmektedirler.[1162] Diğer bir görüşe göre ise 4. fıkra düzenlemesinin 1. ve 2. fıkralarda düzenlenen temel suç tipine bağlılık devam ettiğinden bu düzenleme suçun nitelikli halini oluşturmaktadır.[1163] Koca ve Akbulut' un da belirtmiş olduğu gibi kanaatimizce de 4. fıkra düzenlemesi 1. ve 2. fıkrada düzenlenen suç tiplerinden ayrı ve tüm unsurlarını taşıyan bağımsız bir suç düzenlemesi olup niteliği itibariyle de bileşik suçtur. Zira, 1. veya 2. fıkrada yer alan suçlar, 4. fıkrada yer alan haksız yarar sağlama suçunun unsurunu oluşturması dolayısıyla 4. fıkra tek fiil sayılan bileşik suç olarak kabul edilecektir.

4. fıkrada yer alan düzenlemede "başka bir suçu oluşturmaması"[1164] ifadesi kullanılmış, madde gerekçesinde ise bu ifade ile anlaşılması gerekenin:

> *"Bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir."*[1165]

1162 Bkz. Koca ve Üzülmez, a.g.e., s. 834.
Akbulut' a göre de 4. fıkra, 1. ve 2. fıkralarla aynı maddede düzenlenmişse de faklı bir suç niteliğindedir. Zira ihlal şekilleri ve korunan hukuki değerler aynı olmadığından, 1. ve 2. fıkralarda yer alan suçların temel şeklinin unsurları dışında ilave unsurlar şeklinde değil de başka suçların unsurlarını da kapsayan ve ilave ihlal şekli arayan bir düzenleme niteliğinde olduğundan, ayrıca haksız çıkar sağlamanın 1. ve 2. fıkrada ifade edilen fiillerin sonucunda gerçekleşmesi aranmadığından bu düzenleme 1. ve 2. fıkrada yer alan suçların nitelikli halini ve neticesi sebebiyle ağırlaşmış şeklini oluşturmamaktadır. Bu fıkra ile düzenlenen suç TCK' nın 42. maddesi anlamında bileşik suç niteliği taşımaktadır. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 217, 218.
1163 Özbek, v.d., a.g.e., s. 941; Yaşar, Gökcan ve Artuç, a.g.e., s. 7319.
Karagülmez' e göre ise: "Son fıkrada ise, failin maddede belirtilen fiillere işlemek suretiyle kendisine ya da başkasına haksız bir çıkar sağlaması başka bir suç oluşturmadığı takdirde bu suçlar için de bir ağırlaştırıcı neden olarak öngörülerek cezalandırılmıştır." Bkz. Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 161.
1164 Yargıtay ise bir kararında ifadeyi şu şekilde açıklamıştır:
"TCK'nın 244/4. maddesinde, "Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde…" biçimindeki ifadeden bu fıkradaki düzenlemenin tali norm niteliğinde olduğunun anlaşılması, buna göre öncelikle yasada düzenlenmiş olan bilişim sistemlerinin kullanılması suretiyle işlenebilen diğer suçların oluşup oluşmadığı değerlendirildikten sonra gerçekleştirilen eylem bu suçlardan hiçbirisinin tanımına uygun değil ise, bu durumda eylemin TCK'nın 244/4. maddesi kapsamında suç oluşturacağı düşünülerek; müştekinin ..... Bankasında bulunan hesabına internet üzerinden ulaşan sanığın, müştekinin hesabına girerek 410,00 TL'yi havale yoluyla kendi hesabına havale ettiği, sanığın eylemindeki kastın, müştekinin banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi hesabına geçirmeye, müştekinin rızasına aykırı olarak mal varlığında azalmaya neden olmaya, var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yönelik olması nedeniyle, Yargıtay Ceza Genel Kurulu'nun 17.11.2009 gün ve 193/268 Sayılı kararında açıklandığı üzere; sanığın fiilinin TCK'nın 142/2-e maddesinde öngörülen "bilişim suretiyle hırsızlık" suçunu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi, …" bkz. Yargıtay 17. Ceza Dairesi, 29.2.2016 t., E: 2015/8568, K:2016/2521, https://legalbank.net/arama, ET. 15 Temmuz 2020; Aynı yönde bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 341.
1165 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 221; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 340.

Madde metninde yer alan "başka bir suç oluşturmaması hali" ifadesinin madde gerekçesinde "fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması" ifadesi ile çelişki oluşturduğu görülmekte olup doktrinde madde metninin gerekçeye uygun olarak düzeltilmesi gerektiğini belirten yazarlar[1166] bulunmakta ise de bizim de katılmış olduğumuz diğer görüşe göre esas alınması gereken normun kendisi olduğu için gerekçenin maddeye uygun şekilde düzeltilmesi başka bir deyişle daha ağır cezayı gerektirme hali aranmaksızın gerekçede başka bir suç oluşturmaması halinin kabul edilmesi gerekmektedir.[1167] Zira, Koca' nın da belirtmiş olduğu gibi bu suç "tali norm"[1168] niteliğinde olup tali normlar bu konuda bir boşluk bırakmamak üzere konulan hükümler olduğundan[1169] ve esasen asli normun bulunduğu durumda tali normun olaya uygulanması mümkün olmayacağından burada bilişim sistemi suretiyle dolandırıcılık, bilişim suretiyle hırsızlık, hizmet nedeniyle güveni kötüye kullanma, zimmet vb. başka suçların oluştuğu hallerde 244. m.' nin 4. fıkrasında düzenlenen suç oluşmayacaktır.[1170] Doktrinde bu normun tali norm olarak olarak düzenlenmesinin nedeni olarak sebebi olarak ise sürekli değişen ve gelişen teknoloji sayesinde işlenen suçların cezasız bırakılmaması olduğu[1171] belirtilmekte olup biz de bu görüşe katılmaktayız. Bunun yanında, tali norm olarak düzenlenen bu hükmün uygulanma alanının da çok sınırlı kaldığı söylenebilecektir.[1172]

1166 Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 223.

1167 Aynı yönde bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 340.

1168 Eker' e göre ise: "İlgili madde gerekçesinden anlaşıldığı üzere bu fıkrada düzenleme altına alınan genel nitelikli bir hükümdür; bu yüzden daha özel nitelikteki bir normun saptadığı suç hipotezine uygunluk gösteren bir eylem gündeme geldiği takdirde bu norm değil, özel hüküm uygulanacaktır." Bkz. Eker, a.g.e., s. 127.

1169 Koca ve Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 834, 835.

Özbek, Kanbur, Doğan, Bacaksız ve Tepe' ye göre de: "…Buna göre tali norm sonra uygulanır. Amaç oluşabilecek boşlukları tamamlamaktır. İşte m.244/4'te yer alan bu ifade ile söz konusu hükmün tali bir niteliğe sahip olduğu açıklanmış olmaktadır. Ancak kanımızca bu ifade m.244'ün özel norm olma özelliği ile çelişmektedir." Bkz. Özbek, v.d., a.g.e., s. 942.

Suçun tali norm niteliğinde olduğunu belirten diğer yazarlar için bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 221.

1170 Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 241.

"…fıkra metninde açıkça "başka bir suçu oluşturmaması halinde" denilmesi nedeniyle, kovuşturma konusu eylemin başka bir suçu oluşturması halinde bu fıkranın tatbiki imkânı bulunmamaktadır. Diğer bir deyişle, bir eylem hem dördüncü fıkradaki suçu hem de başka bir suçu oluşturuyorsa, artık fikri içtima kurallarına gidilmeksizin diğer hükmün tatbiki gerekir…diğer suçun cezasının "daha ağır ya da hafif olması dikkate alınmaksızın ", somut olayda diğer suç uygulanacaktır." Bkz. A.e., s. 249.

Soyaslan' a göre ise: "…Ancak fiilin suç oluşturması için başka bir düzenleme ile daha ağır cezayı gerektiren bir suç olmamalıdır. Söz konusu suç zimmet, dolandırıcılık, hırsızlık ve güveni kötüye kullanma olabilir." Bkz. Soyaslan, a.g.e., s. 651.

1171 Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 250.

1172 Doğan, a.g.e., s. 156; Yılmaz, a.g.e., s. 94, 95.

4. fıkrada düzenlenmiş olan suç tipi, 765 sayılı TCK' nın 525 b/2 m.' sinde "bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlamak", "banka ve kredi kartlarını kötüye kullanmak", "bilişim sistemleri aracılığıyla dolandırıcılık" ve "bilişim sistemleri aracılığıyla hırsızlık" fiilleri geniş bir şekilde düzenlenmişken 5237 sayılı TCK' nın 4. fıkrasında "bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlamak" fiili suç olarak düzenlenerek bu suçun nasıl gerçekleştirileceği[1173] başka bir deyişle suçu oluşturan fiiller açıkça gösterilmiş ve suçun sınırları eski TCK' da yer alan hükme göre daha iyi çizilmiştir.[1174] Bunun yanında AKSS' nin "bilgisayarla bağlantılı dolandırıcılık" başlıklı 8. m.' sinde, *"kendisi veya bir başkasına haksız menfaat sağlamak amacıyla, bilişim sisteminde yer alan verilere herhangi bir şekilde yeni veriler ekleme, verileri herhangi bir şekilde değiştirme, silme veya erişilemez kılma, sistemin işleyişine engel olma"*[1175] fiillerinin cezalandırılması hükme bağlanmış olup 244. m.' nin 4. fıkrasında yer alan suç ile sözleşme hükmünün uyumlaştırılmasının sağlandığı söylenebilmektedir.[1176]

3.2.2.9.1. Korunan Hukuksal Değer

Doktrinde, 244. m.' nin 4. fıkrasında düzenlenmiş olan suçla korunan hukuksal değerin malvarlığı olduğunu belirten yazarların[1177] yanında fail tarafından zarara uğratılan veya elde edilen maddi ya da manevi her türlü hak ya da yarar olduğunu belirten yazarlar[1178] da bulunmaktadır. Kanaatimizce de, suç tipinde "haksız çıkarın

1173 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 340.

1174 Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 238, 239.

1175 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6937; Doğan, a.g.e., s. 145, 146.

1176 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6937.
Ancak Akbulut' un da belirtmiş olduğu gibi: "…Düzenlememizde Sözleşmede yer alan suçun maddi menfaat sağlamak amacıyla gerçekleştirilmesi aranmamış onun yerine haksız çıkar sağlanması ifade edilmiştir. Çıkarın maddi nitelikte olmasına ilişkin bir belirleme yapılmamıştır. Ayrıca mal kaybına sebebiyet verilmesi yani zarara neden olunması Sözleşmenin aksine TCK m. 244/4'te yer almamıştır. Ayrıca hile veya sahtekârlık niyetiyle fiillerin gerçekleştirilmesi de Ceza Kanunumuzdaki düzenlemede hükme bağlanmamıştır." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 220.

1177 "Suçun oluşabilmesi için bilişim sisteminin işleyişinin engellenmesi veya sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi ya da başka yere gönderilmesi suretiyle haksız yararın sağlanması gerektiği için bu suçla hem 244. maddenin 1. ve 2. fıkralarının koruduğu hukuki değerlerin, hem de malvarlığı hukuki değerlerinin birlikte korunduğu söylenebilir. Ancak bu değerlerden ağırlıklı olanı kişilerin malvarlığıdır. Zira bilişim sistemi malvarlığı değerlerine yönelik saldırıda bir araç fonksiyonu görmektedir." Bkz. Koca ve Üzülmez, a.g.e., s. 839.
Akbulut' a göre de korunan değer malvarlığı olup dolaylı olarak TCK'nın 244/1-2' de düzenlenen suçların koruduğu hukuki değerler de korunmaktadır. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 230.

1178 Doğan, a.g.e., s. 146; Soyaslan, a.g.e., s. 651.
Artuk, Gökcen ve Yenidünya' ya göre de: "Suç tipinde korunan hukuksal değer, kişilerin özel hayatlarının gizliliğinden, malvarlığı haklarının korunmasına kadar geniş çerçevede ele alınabilir. Burada bilişim sistemlerine haksız müdahalelerde bulunarak kişilerin maddi ve manevi haklarına

sağlanması" unsuru açıkça malvarlığı hakkı ile sınırlandırılmamış olmadığından suçla korunan hukuksal değer için, mağdurun zarara uğraması karşısında ekonomik değer taşıyan maddi hakları olabileceği gibi ekonomik bir değer taşımayan itibar kaybı, kişilik hakları gibi manevi hakkı da kabul edilebilecek olup doktrinde de belirtildiği üzere suç tipinde 1. ve 2. fıkralarda yer alan fiillerin gerçekleştirilmesi arandığından bu suçlar ile korunan hukuksal değerlerin de ayrıca ve geniş anlamda korunduğunu değerlendirmekteyiz. Nitekim, kanun koyucunun 4. fıkra düzenlemesini, tali nitelikte bir norm olarak düzenlemiş ve kanaatimizce boşluk bırakmamak adına da "haksız çıkar" ifadesini kullanmıştır. Ancak Dülger' in de belirtmiş olduğu gibi[1179] uygulamada genellikle suçun konusunu da oluşturan bu değer olarak mağdurun malvarlığı hakkından olan maddi hakları ile karşılaşılmaktadır.

3.2.2.9.2. Maddi Unsur

3.2.2.9.2.1. Fail ve Mağdur

Madde düzenlemesinde fail için herhangi ayırıcı bir özellik aranmadığından herkes bu suçun faili olabilecek[1180] olup 1. ve 2. fıkralarda yer alan suç tipinin fail başlığı altında belirtmiş olduğumuz hususlar burada da geçerlidir. Ayrıca, TCK' nın

---

yapılan saldırılar önlenmek istenmiştir." Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6937, 6938. Aynı yönde bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 241.

Dülger' e göre de suçun oluşması için gereken haksız yararın türü bakımından ayrım yapılmadığından fail tarafından elde edilen maddi ya da manevi her türlü yarar suçla korunan hukuksal değeri oluşturmaktadır. "…İnceleme konusu suç tipini oluşturan eylemlerin gerçekleştirilmesi nedeniyle mağdurun malvarlığında bir zararın meydana gelmesi durumunda ise genellikle ya nitelikli dolandırıcılık suçu ya da nitelikli hırsızlık suçu gerçekleşmiş olur. Bu iki suçtan birinin oluşmaması halinde ise, 244/4 söz konusu olabilir. Dolayısıyla sağlanan haksız yararının maddi bir yarar olmaması halinde 244/4'ün devreye girmesi pekala mümkündür. Dolayısıyla bu suç tipinin yeni düzenlemesi karşısında suçla korunan hukuksal değerin mağdurun manevi bir hakkının olması da olanaklıdır. Ancak ilk paragrafta da belirttiğimiz üzere, suç tipinde kuramsal olarak bu yönde bir sınırlama olmamakla birlikte uygulamada genellikle suçun konusunu da oluşturan bu değer bir malvarlığı hakkıdır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 341, 342.

1179 A.e., s. 342.

1180 Koca ve Üzülmez, a.g.e., s. 839; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6939; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 243; Soyaslan, a.g.e., s. 651; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 342; Doğan, a.g.e., s. 147.

"…suçun faili, veriler üzerinde tasarruf yetkisine sahip olmayan kişi, sistemin sahibi olmayan kişi ya da kullananın dışındaki herhangi bir kişi olabilir. Veriler üzerinde tasarruf yetkisine sahip kişi ile sistemin sahibi farklı bir kişi ise sistem sahibi de 4. fıkradaki suçu işleyebilir. Tasarruf yetkisine sahip olmayıp yalnızca kullanım yetkisine sahip kişi de TCK'nın 244. maddesinin 4. fıkrasındaki suçun faili olabilir. Sistemin sahibi ile kullananın farklı olması durumunda sistemi kullanma yetkisine sahip kişi de 4. fıkradaki suçu gerçekleştirebilir." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 231.

246. m.' si gereğince, yararına haksız menfaat sağlanan tüzel kişi ise bunlara özgü güvenlik tedbirlerine hükmolunacaktır.

Suçun mağduru bakımından da ayrıca bir özellik aranmadığından bu suçun mağduru herkes olabilir.[1181] Ancak doktrinde bazı yazarlara göre suçun mağduru failin müdahalede bulunduğu ve bu suretle haksız çıkar sağladığı bilişim sisteminin veya verinin sahibidir.[1182] Bir başka görüşe göre bu suçun mağdurunu bilişim sisteminin maliki veya zilyedi ile sınırlamak mümkün olmayıp verilerin maliki dahi olunması gerekmemektedir, bu bağlamda verinin ilgilisi olma mağdur olmak için yeterlidir.[1183] Bir diğer görüşe göre ise elde edilen çıkar dolayısıyla malvarlığında azalma olan herkes bu suçun mağduru olabilecektir.[1184] Yargıtay ise internet aracılığı ile hesaptan havale yapılması işlemlerinde sadece hesap sahiplerini suçun mağduru olarak kabul etmekte, bankanın doğrudan suçtan zarar görmediğini belirtmektedir.[1185]

1181 Koca ve Üzülmez, a.g.e., s. 839; Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345, s. 6939*; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 243; Soyaslan, a.g.e., s. 652; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 342; Akbulut, *Bilişim Alanında Suçlar*, s. 232.

1182 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6939; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 242.

1183 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 342, 343; Soyaslan, a.g.e., s. 652.
"Örneğin bir internet servis sağlayıcısından aldığı erişim, teknik destek ve veri taşıma/depolama hizmetiyle (host) üyelerine günlük ekonomi haberlerini ve tahminleri ileten bir internet sitesinde bulunan verilerin, rakip site tarafından değiştirilmesi yoluyla yanlış haber ve değerlendirilmelerin girilmesi sonucu güvenilirliğinin zedelenmesi ve böylece rakip site tarafından haksız yarar sağlanması durumunda, ekonomi haberleri veren site ne bilişim sisteminin ne de verilerin malikidir ancak mağdur durumundadır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 343.
Doğan' a göre de: "Kanaatimizce bu suçun işlenmesi nedeniyle zarar gören herkes bu suçun mağduru olabilir." Bkz. Doğan, a.g.e., s. 147.

1184 "Bilişim sistemleri aracılığıyla malvarlığında azalma meydana gelen gerçek kişiler bu suçun mağdurudurlar. Suçun bileşik suç olması nedeniyle bilişim sisteminin işleyişi engellenen veya sistemdeki verileri zarar gören kişilerin de malvarlığı üzerinde tasarrufta bulunan kişilerden farklı kişiler olması halinde, mağdur olacağı kabul edilmelidir." Bkz. Koca ve Üzülmez, a.g.e., s. 839. Aynı yönde bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 232, 233.

1185 Akbulut, *Bilişim Alanında Suçlar*, s. 233.
Yargıtay 2. Ceza Dairesi bir kararında: "… Sanıklar hakkında müşteki...'ın ...A.Ş şubesinde bulunan hesaptan, aynı bankanın bir başka şubesindeki hesabına internet aracılığıyla 16.500 TL tutarında havale ettiği iddiasıyla açılan kamu davasında müşteki bankanın doğrudan suçtan zarar görmediği ve mahkemece katılma kararı verilmiş olması da hükmü temyiz hakkı vermeyeceğinden katılan vekilinin temyiz isteminin CMUK'nın 317. maddesi uyarınca istem gibi REDDİNE," Bkz Yargıtay 2. Ceza Dairesi, 1.6.2016 t., E:2014/25924, K:2016/10421, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay 11. Ceza Dairesi'nin, 27.9.2007 tarihli, E: 2007/6709, K: 2007/6012 sayılı kararında: "Somut olayda; sanığın, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri) sahte kimliklerle açtırdığı hesaplara internet yoluyla göndererek, yine sahte kimliklerle bu paraları çekmek istemesinden ibaret eylemlerinin; paranın sanığın açtırdığı hesaplara intikaline kadar gerçek kişilere yöneltilmiş hile bulunmayıp eylemlerin tamamen bilişim sistemi içinde gerçekleştirildiğinden, her bir mağdura karşı işlenmiş ayrı ayrı 5237 sayılı TCK.nun 244/4 maddesine uyan suçu oluşturduğu ve paranın açtırdığı hesaplara transferiyle suçun tamamlanacağı gözetilmeden, suçun vasıflandırılmasında yanılgıya düşülerek nitelikli dolandırıcılığa teşebbüs suçundan mahkûmiyet hükmü kurulması" şeklinde karar verilmiştir. Aynı yönde bkz. Yargıtay 8.

Kanaatimizce, 4. fıkrada düzenlenen suç haksız yararın sağlanması ile gerçekleştirildiğinden ve bu yarar karşılığında mağdur sıfatı bulunacak kişilerde de bir zararın gerçekleşmesi gerekmektedir. Zira Yargıtay' ın da mağdur sıfatını belirlerken zarara uğrama kriterini esas aldığı söylenebilecektir. Korunan hukuksal yarar başlığı altında da belirtmiş olduğumuz ve doktrinde yer alan 2. görüşte belirtildiği gibi bu suç bakımından maddi veya manevi zarara uğramış olmak şartı ile ilgili olan herkes bu suçun mağduru olabilecektir. Dolayısıyla bu suç bakımından mağdurun, bilişim sistemi veya verinin sahibi olarak kabul edilmesi yerine bunlar üzerinde hak sahibi olma kavramının benimsenerek[1186] ve buna göre belirleme yapılması daha uygun olacaktır.

3.2.2.9.2.2. Suçun Konusu

Suçun maddi konusunu failin sağladığı "haksız çıkar" veya "hukuka aykırı yarar" oluşturmaktadır. Ancak doktrinde bu konuda fikir ayrılığı bulunmaktadır. Doktrinde yer alan bir grup yazara göre, bu suçun konusunu "hukuka aykırı yarar" oluşturup bu yarar ekonomik değeri olan mali bir yarar olabileceği gibi ekonomik bir getirisi ve değeri olmayan tamamen tatmine yönelik manevi her türlü yarar da olabilecektir.[1187] Çıkar kavramını geniş yorumlayanların, TCK m. 244/4 hükmünün AKSS' de karşılığını oluşturan 8. m.' sinde yaptırıma bağlanan "haksız yere maddi menfaat" ifadesinin TCK' da "haksız bir çıkar" olarak kabul edilerek bir kısıtlamaya yer verilmemesini, maddi veya manevi her türlü çıkarın bu hüküm kapsamına girebileceği şeklinde açıklamış oldukları belirtilmektedir.[1188] Diğer bir görüşe göre ise suçun konusu, malvarlığına ilişkin herhangi bir değer başka bir deyişle kişilerin ekonomik durumunda doğrudan veya dolaylı olarak iyileşme meydana getiren herhangi bir menfaat oluşturmaktadır.[1189] Artuk-Gökcen-Yenidünya ise, bu suçun

Ceza Dairesi, 31.5.2017 t., E: 2017/7519, K:2017/6376, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1186 Doğan, a.g.e., s. 147.

1187 Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 243; Doğan, a.g.e., s. 147; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 343; Soyaslan, a.g.e., s. 652; Özbek, v.d., a.g.e., s. 946.

1188 Karagöz, a.g.e., s. 132.

1189 Koca ve Üzülmez, a.g.e., s. 839; Akbulut, *Bilişim Alanında Suçlar,* s. 234.
"Bu anlamda failin kendisinin veya başkasının malvarlığında artışa veya borçlarında azalmaya yol açan her türlü kazanç bu suça konu olabilecektir. Keza kişinin bilişim sistemine yaptığı haksız müdahale nedeniyle işe alınması, işinde terfi etmesi, bir ihaleyi alması gibi hallerde de çıkar sağlandığı kabul edilmelidir. Ekonomik olarak ölçülemeyen ve yalnızca kişilerde manevi tatmin duygusu meydana getiren haz veya manevi yararın bu suça konu olamayacağını düşünüyoruz." Bkz. Koca ve Üzülmez, a.g.e., s. 839, 840.

konusunun bilişim sistemi veya sistemdeki veriler olduğunu belirtmektedir.[1190] Yargıtay' ın ise bilişim sistemindeki verilerini değiştirmek suretiyle ders notlarını ve devamsızlık durumlarını değiştirdiklerinden bahisle sanıklar hakkında açılan bir davada, bilişim sisteminde yapılan işlemler sonucu devamsızlık ve not düzeltmelerin dışında sağlandığı belirtilen haksız menfaatlerin ne olduğunun ayrıca açıklanması gerektiğini belirterek yetersiz gerekçe sebebiyle ilk derece Mahkemesi' nin 244/4. m.' sinin olaya uygulanması yönünde vermiş olduğu kararın bozulmasına hükmetmiştir.[1191]

Kanaatimizce, 4. fıkranın mevcut düzenlemesi uyarınca suçun konusu ekonomik değeri olan maddi bir yarar olabileceği gibi ekonomik bir getirisi ve değeri olmayan itibar kaybı, kişilik haklarına müdahale gibi manevi yarar da oluşturabilmektedir. Zira, korunan hukuksal değer başlığında da belirtmiş olduğumuz üzere, suç tipinde "maddi menfaat" olarak bir sınırlama getirilmemiş olduğundan Yargıtay kararlarında da belirtildiği üzere her somut olayda haksız yararın somut bir şekilde belirlenmesi suretiyle manevi yararlar da bu suçun konusunu oluşturabilecektir.[1192] Ancak belirtmek gerekir ki, 1. ve 2. fıkrada yer alan suçların her işlenişinde failin az ya da çok manevi bir tatmini gerçekleştireceği düşünüldüğünde

1190 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6939.

1191 "Kabule göre de;
a) Sanıkların okul ders notlarını ve devamsızlık durumlarını değiştirmek için bilişim sisteminin Milli Eğitim Bakanlığı'na bağlı okullarda kullanılan e-okul bilişim sistemi şifreleri ele geçirmek suretiyle yükletilen suçu işledikleri kabul edilmesi nedeniyle hükmolunan cezasının sitenin kamu kurumuna ait olması nedeniyle TCK.nun 244/3. maddesi gereğince cezaların arttırılması gerektiği gözetilmeden yazılı şekilde hükümler kurulması,
b) Bilişim sisteminde yapılan işlemler sonucu devamsızlık ve not düzeltmelerin dışında sağlandığı belirtilen haksız menfaatlerin ne olup kim tarafından sağlandığı karar yerinde açıklanıp tartışılmadan yetersiz gerekçe ile yazılı şekilde TCK.nun 244/4. maddesinin uygulanması, … BOZULMASINA" bkz. Yargıtay 8. Ceza Dairesi, 15.2.2017 t., E: 2016/3794, K: 2017/1405, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay' ın bir başka kararında: ""www..com" adlı sitenin sahibi olan sanığın, katılana ait internet sitesini erişilmez kılarak ne suretle yarar sağladığı karar yerinde gösterilip tartışılmadan TCK.nun 244/2. maddesi yerine aynı maddenin 4. fıkrası uyarınca hüküm kurulması, … (BOZULMASINA)" hükmetmiştir. Bkz. Yargıtay 8. Ceza Dairesi, 26.11.2014 t., E: 2014/27215, K: 2014/28029, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay yeni tarihli bir kararında, sanığın haksız bir menfaat temini olup olmadığının, olmuş ise ne şekilde ve ne miktarda menfaat temin ettiğinin denetime olarak verecek şekilde kesin olarak tespitinden sonra hukuki durumunun tayin ve takdiri gerektiği gözetilmeden, eksik inceleme ve araştırma sonucu yazılı şekilde hükümler kurulması sebepleriyle yerel mahkeme kararının bozulmasına hükmetmiştir. Bkz. Yargıtay 15. Ceza Dairesi, 23.10.2019 t., E:2017/4738, K: 2019/10423, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1192 Yargıtay 11. Ceza Dairesi' nin 15.1.2013 tarihli, E: 2010/12162, K: 2013/658 sayılı kararında: ' "Trafik görevlilerinin yaptığı alkol muayenesine itiraz üzerine Devlet hastanesine götürülen ve kan numunesi alınan kişinin yakını olan hastane otomasyon sorumlusunun, akrabası olan kişinin ceza almasını ve ehliyetine el konulmasını engellemek amacıyla hastane bilişim sistemine hukuka aykırı olarak müdahale etmesini TCK 244/4. madde kapsamında" kabul eden yerel mahkeme kararını yerinde bulmuştur.' (*Aktaran* Gül, a.g.e., s. 96).

manevi tatmin gibi somut olarak belirlenemeyecek ve yeterli olmayan manevi yararların bu suçun konusunu oluşturduğu kabul edilmemelidir. Zira, böyle bir halin kabulünün normun tamamlayıcı niteliği ile çelişeceği düşünülmektedir.

3.2.2.9.2.3. Fiil

244. m.' nin 4. fıkrasında yer alan suç, 1. ve 2. fıkralarda düzenlenen suç tipinde yer alan fiillerin işlenmesi suretiyle ve bunun yanında haksız yarar sağlanması şartı ile gerçekleşebildiğinden birden çok hareketli ve "bağlı hareketli suç"[1193] niteliği taşımaktadır.[1194] Bunun yanında, çıkar sağlamaya yönelik 1. ve 2. fıkrada yer alan hareketler ise seçimlik olarak düzenlendiğinden ve bunlardan birinin veya birkaçının gerçekleştirilmesi ile haksız yararın elde edilmesi anında tek bir suç oluşacağından aynı zamanda seçimlik hareketli suç söz konusudur.[1195] Bunun dışında, söz konusu suç tipini oluşturan 244. m.' nin 1. ve 2. fıkralarındaki fiiller hakkında ilgili başlıklar altında yapmış olduğumuz açıklamalar bu suç açısından da geçerli olduğundan bu başlık altında ayrıca bir açıklama yapılmayacaktır.

Fıkrada düzenlenen suçun oluşabilmesi için haksız çıkarın elde edilmiş olunması şartı arandığından bu suç için neticeli bir suç diyebilmekteyiz. Haksız çıkar kavramı ile ifade edilenin "hukuka aykırı yarar" olduğu belirtilmekte[1196] olup hukuken tasvip edilmeyen her türlü menfaat, haksız çıkar kavramı içinde mütalaa edilebilmektedir.[1197] Her ne kadar doktrinde bu suçun oluşabilmesi için "haksız çıkar" veya "hukuka aykırı yarar" karşılığında zarara uğranmış olunması şartı aranmadığını

1193 Ancak Apaydın' a göre, "Fail serbest olarak herhangi bir harekette bulunduktan sonra TCK'nın 244/1'inci maddesi ve fıkrası gereği bilişim sistemini engelleyip veya bozarak kendisinin ya da başkasının yararına haksız bir çıkar sağlarsa artık eylem başka bir suçu oluşturmuyorsa, TCK'nın 244/4'üncü maddesi ve fıkrası hükmünün tatbiki gerekecektir." Bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 243.
1194 Koca ve Üzülmez, a.g.e., s. 840; Akbulut, *Bilişim Alanında Suçlar,* s. 234.
1195 Akbulut, *Bilişim Alanında Suçlar*, s. 234, 235; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 344; Soyaslan, a.g.e., s. 652; Doğan, a.g.e., s. 148.
1196 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 348; Doğan, a.g.e., s. 148.
1197 Koca ve Üzülmez, a.g.e., s. 840; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 243; Doğan, a.g.e., s. 149.

belirten yazarlar[1198] bulunmakta ise de bizim de katılmış olduğumuz diğer görüşe[1199] göre, her ne kadar fıkra düzenlemesinde "zarar" ifadesi kullanılmamışsa da failin kendisinin veya başkasının yararına çıkar sağlaması suretiyle mağdura bir zarar vermiş olması gerekmektedir. Zira, suç 1. ve 2. fıkrada yer alan fiillerle gerçekleştirilmekte ve bu fiilleri incelerken de belirtmiş olduğumuz gibi bu fiillerle oluşan suçlar da zarar suçu niteliğindedir. Bunun yanında, Yargıtay uygulamasına bakıldığında da mağdur sıfatı belirlenirken bu fiiller sonucu elde edilen haksız yarar karşılığında zarara uğrayan kişi veya kişiler belirlenmektedir. O halde bu fıkrada yer alan suçu zarar suçu olarak değerlendirmekteyiz.

3.2.2.9.3. Manevi Unsur

Söz konusu suçun ancak kasten işlenebilen bir suç olup suçun taksirle işlenebilen hali düzenlenmediğinden bu suç taksirle işlenemeyecektir.[1200] Doktrinde manevi unsur açısından, suç tipinde "haksız çıkar" sağlamak düzenlendiğinden suçun oluşabilmesi için failin sağladığı çıkarın haksız olduğunu da bilmesi gerektiğinden bu suçun ancak doğrudan kastla işlenebileceğini belirten yazarların[1201] yanında failin genel suç işleme kastının yanında özel bir kasta da sahip olması gerektiğini belirten yazarlar[1202] bulunduğu gibi, failin suç işlemeye yönelik genel kastının yeterli olduğunu

1198 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 349; Soyaslan, a.g.e., s. 652; Doğan, a.g.e., s. 149;
"Failin kendisine veya başkasına çıkar sağlaması suçun oluşması için yeterli olup, mağdurun bu fiil nedeniyle zarara uğraması aranmaz. Ancak bu durum suçun zarar suçu olarak nitelendirilmesine engel değildir." Bkz. Koca ve Üzülmez, a.g.e., s. 840.
"Kanaatimizce TCK'nın 244/4'üncü maddesindeki suçun gerçekleşmesi için zararın oluşması gerekmediği için, diğer koşulların oluşması ile birlikte failin haksız bir yarar elde etmesi suçun oluşumu açısından yeterli olduğundan, suç zarar suçu olmayıp tehlike suçudur. Çünkü failin hukuka aykırı yarar elde etmesi sonucu, suçla korunan hukuki değerler olan bireylere ait bilişim sistemlerinin işleyişi ve güvenliği ile iletişim ve mülkiyet haklarının korunması ihlal edilerek tehlikeye sokulmaktadır." Bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 246.
1199 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6939; Akbulut, *Bilişim Alanında Suçlar,* s. 235.
Ancak Akbulut' a göre zarar, malvarlığında meydana gelen kayıp şeklinde olması gerekirken biz buna katılmamaktayız. Zira "haksız çıkar" kavramını açıklarken de belirtmiş olduğumuz üzere maddi veya manevi olabileceği gibi zararın da maddi veya manevi olabileceğini kabul etmekteyiz.
1200 Koca ve Üzülmez, a.g.e., s. 841; Akbulut, *Bilişim Alanında Suçlar*, s. 260; Doğan, a.g.e., s. 149.
1201 "…suçun oluşabilmesi için failin sağladığı çıkarın haksız olduğunu bilmesi de gerekir. Burada çıkarın haksızlığına ilişkin bilgi kastın kapsamında mütalaa edilmelidir." Bkz. Koca ve Üzülmez, a.g.e., s. 841. Aynı yönde bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 260, 261.
1202 Kurt, a.g.e., s. 175; Taşkın, a.g.e., s.59; Doğan, a.g.e., s. 149.
Artuk, Gökcen ve Yenidünya'ya göre ise: "Kanunda saike (maksada) işaret eden herhangi bir ibare yer almamakla birlikte, 4 üncü fıkradaki düzenlemenin, 1 inci ve 2 nci fıkralar yönünden farkını ortaya koyabilmek ile suça teşebbüs konusunda doğru sonuçlara ulaşabilmek adına, sisteme haksız

bu bağlamda suçun olası kastla da işlenebileceğini belirten yazarlar[1203] da bulunmaktadır.

Kanaatimizce, Erdoğan' ın da belirtmiş olduğu gibi 4. fıkrada yer alan suç tipi düzenlemesinde ayrıca bir saike (amaca) yer verilmediğinden burada özel kastın varlığının aranmasından bahsedilemeyecek olup bu suçun işlenilmesi bakımından genel kastın varlığı kabul edilebilecektir. Zira, Dülger' in de belirtmiş olduğu gibi suç tipinde yer alan haksız çıkarın sağlanması ifadesi suçun maddi unsurunda yer alan neticeye yönelik bir ifadedir. Dolayısıyla burada failin amacına yönelik bir belirleme yapılmamıştır. Ancak failin suç işlemeye yönelik genel kastı kapsamında neticenin yani sağladığı veya elde ettiği çıkarın haksız başka bir deyişle hukuka aykırı olduğunun bilincinde olması gerekmektedir. Bu yönüyle bu suç yönünden failin doğrudan veya olası kast ile hareket edebileceği kabul edilmelidir.

3.2.2.9.4. Hukuka Aykırılık

4. fıkrada yer alan suçun unsurları için 1. ve 2. fıkraya atıf yapıldığından ilk iki fıkra için belirtmiş olduğumuz hukuka uygunluk sebepleri bu suç için de geçerli[1204] olmakla birlikte madde metninde failin kendisinin veya başkasının yararına haksız çıkar sağlaması arandığından rızanın varlığı halinde hukuka aykırılığın ortadan

---

çıkar sağlamak kastıyla müdahalede bulunulması aranır." Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6939.

1203 Soyaslan, a.g.e., s. 653.

"Kanaatimizce bu suçta kast yeterlidir…kanun metninde bulunan "kendisinin veya başkasının yararına haksız bir çıkar sağlamasının" şeklindeki cümlenin saike işaret ettiği akla gelebilir ise de; saikin arandığının kabul edilebilmesi için kanun metninde açıkça saike, yani amaca dair bir ibare bulunması gerekmektedir. Örneğin TCK'nın 105'nci maddesinde cinsel taciz suçu düzenlenirken "cinsel amaçlı olarak", "4"'inci maddesinde hırsızlık suçu düzenlenirken "kendisine veya başkasına bir yarar sağlamak maksadıyla" denilmiştir…" bkz. Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 257.

"…Dikkat edilirse suç tipinde yer alan "kişinin kendisinin veya başkasının yararına haksız çıkar sağlaması" ifadesi suçun maddi unsurunda yer alan neticeye yönelik bir ifadedir. Bir başka deyişle yasa koyucu bu ifadeye yer vermekle failin gerçekleştirdiği eylem neticesinde kendisinin veya başkasının yararına haksız çıkar sağlama neticesinin gerçekleştirilmesini aramış, failin hangi amaçla hareket ettiğini önemsememiştir…örneğin sırf mağdurun bilişim sistemine zarar vermek amacıyla hareket etmesi ancak bu zararın neticesinde müşterilerin çökertilen siteye giremeyip failin sahibi olduğu siteye yönelip buradan alışveriş yapmaları neticesinde failin bundan bir yarar elde etmesi halinde 244/4 uygulanır; çünkü suç tipinde failin amacı değil, eylemi sonucunda gerçekleşen netice suçun oluşması için aranır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 351.

"…Suç tipinde failin amacına ya da derin maksat anlamına gelen saike yönelik bir ifade bulunmamakta olup, yasa koyucu failin gerçekleştirdiği eylem neticesinde kendisinin veya başkasının yararına haksız çıkar sağlama neticesinin gerçekleştirmesini aramış, failin hangi saikle hareket ettiğini önemsememiştir." Bkz. Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 246.

1204 Doğan, a.g.e., s. 150.

kalkacağını[1205] ayrıca belirtmek isteriz. Rızanın varlığının ve rıza verenin yetkili olup olmadığının her somut olayda araştırılması gerekmekle birlikte rıza veren malik olabileceği[1206] gibi mağdur başlığı altında da belirtmiş olduğumuz gibi sistem veya veriler üzerinde hak sahibi olan kişinin rızası da geçerli kabul edilmelidir.

3.2.2.9.5. Suçun Nitelikli Hali (Suçun Terör Amacıyla ve Terör Örgütünün Faaliyeti Çerçevesinde İşlenmesi)

244. m.' nin 1. ve 2. fıkralarının nitelikli halinde de belirtilmiş olunduğu üzere, 3713 sayılı Terörle Mücadele Kanunu' nun 4. m.' si[1207] uyarınca 5237 sayılı TCK' nın "Bilişim Alanında Suçlar" bölümünde yer alan 243 ve 244. m.' lerindeki suçların TMK' nın 1. m.' sinde belirtilen terör amacıyla, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlenmesi halinde terör suçu sayılacağı belirtilmiş olduğundan ve 4. fıkra düzenlemesi de bu kapsamda yer aldığından söz konusu Kanun' un 5. m.' sine göre, suçun terör amacıyla işlenmesi hali cezayı artıran nitelikli hal olarak kabul edilecektir.

3.2.2.9.6. Kusurluluk

Söz konusu suç tipi kusurluluk açısından ayrı bir özellik arz etmemektedir.

3.2.2.9.7. TCK madde 244/4 ile Diğer Suçlar Arasındaki İlişki

TCK'nın 243. m.' sinin işlenmesi suretiyle 244. m.' nin 4. fıkrasında yer alan suçun gerçekleştirilmesi halinde 244. m.' nin 1. ve 2. fıkraları başlığı altında da belirtmiş olduğumuz üzere geçit suçu oluşabilecek ve bu durumda faile sadece 244. m.' nin 4. fıkrasından ceza verilecektir.[1208]

1205 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 351; Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 246.

1206 Doğan, a.g.e., s. 150.

1207 "Madde 4 –(Değişik: 29/6/2006-5532/3 md.)Aşağıdaki suçlar 1 inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır:a) Türk Ceza Kanununun 79, 80, 81, 82, 84, 86, 87, 96, 106, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 142, 148, 149, 151, 152, 170, 172, 173, 174, 185, 188, 199, 200, 202, 204, 210, 213, 214, 215, 223, 224, 243, 244, 265, 294, 300, 316, 317, 318 ve 319 uncu maddeleri ile 310 uncu maddesinin ikinci fıkrasında yer alan suçlar…" bkz. https://mevzuat.gov.tr/mevzuatmetin/1.5.3713.pdf 23, ET. Mart 2010.

1208 Doğan, a.g.e., s. 152; Soyaslan, a.g.e., s. 653.
Ancak Koca' ya göre: "Bu suçu işlemek için failin sisteme girmesi zorunlu olduğundan ayrıca 243. maddedeki suç da oluşacaktır. Ancak burada ayrı neviden fikri içtimaın varlığı nedeniyle fail yalnızca 244. maddenin 4. fıkrasından dolayı cezalandırılmalıdır." Bkz. Koca ve Üzülmez, a.g.e., s. 842.

TCK'nın 244. m.' sinin 4. fıkrasındaki suç ile 1. ve 2. fıkralarında yer alan suçlar arasındaki ilişkiye bakıldığında biz 4. fıkranın bileşik suç olduğunu kabul ettiğimizden suçu işleyen failin ayrıca 1. veya 2. fıkra kapsamında cezalandırılmayacağını düşünmekteyiz.[1209]

Doktrinde bu suçun, hırsızlık ve dolandırıcılık gibi suçlardan ayrı olarak düzenlenmesinin, özellikle bilişim sistemleri aracılığıyla hileli veya aldatıcı hareketler yapılarak haksız çıkar sağlanmasında hileli veya aldatıcı hareketlerin kişiye karşı yapılmaması sebebiyle bu eylemin kişiye karşı yapılmasını zorunlu unsur olarak düzenleyen dolandırıcılık suçunun tanımına uymaması ikinci olarak da klasik suçlar olan dolandırıcılık, hırsızlık, güveni kötüye kullanma suçlarında maddi malvarlığı olan şeylerin elde edilmesine karşın bu suçta soyut bir varlık olan verinin ele geçirilmesi olduğu belirtilmektedir.[1210]

Yargıtay Ceza Daireleri ilk uygulamalarında 4. fıkranın sıkça uygulanmasına yol açacak şekilde yoruma girmiş ve uygulamada sıklıkla karşılaşılan internet bankacılığı kullanılmak suretiyle havale işlemlerinde 11. Ceza Dairesi ile 6. Ceza Dairesi arasında benzer eylemler hakkında farklı kararlar verilmişken[1211] Yargıtay

---

1209 Aynı yönde bkz. Koca ve Üzülmez, a.g.e., s. 842; Akbulut, *Bilişim Alanında Suçlar*, s. 263. "Zira bu fıkradaki suçlar, 4. fıkradaki suçun unsuru olduğu için ortada hukuken tek fiil ve tek suç bulunmaktadır (m. 42)." Bkz. Koca ve Üzülmez, a.g.e., s. 842.
Artuk, Gökcen ve Yenidünya' ya göre de: "244/4'te yer alan fiilin gerçekleşmesi halinde, artık fail 244/2 veya 244/3'ten cezalandırılmaz." Bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6940. Aynı yönde bkz. Mahmutoğlu, a.g.e., s. 870. Ancak Yargıtay 15. Ceza Dairesi, hazır beton santralinde müdür olarak görev yapan ve şirketin beton üretimi ve satımı işlemlerinde kullandığı bilişim sisteminde üretime ilişkin datalar ile irsaliye kayıtlarını sisteme haksız bir biçimde girmek suretiyle silen sanığın haksız bir menfaat temini olup olmadığının, olmuş ise ne şekilde ve ne miktarda menfaat temin ettiğinin denetime olarak verecek şekilde kesin olarak tespitinden sonra hukuki durumunun tayin ve takdiri gerektiği gözetilmeden, eksik inceleme ve araştırma sonucu yazılı şekilde hükümler kurulması ve Bilişim sisteminin kamu kurum ya da kuruluşuna ait olmadığı gözetilmeden, sanığın cezasının TCK'nın 244/3. maddesi uyarınca artırılması sebepleriyle yerel mahkeme kararının bozulmasına hükmetmiştir. Bkz. Yargıtay 15. Ceza Dairesi, 23.10.2019 t., E:2017/4738, K: 2019/10423, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yaşar, Gökcan ve Artuç'a göre de: "Failin, birinci ve ikinci fıkradaki hareketleri yapma amacı haksız çıkar sağlamak ise, bu durumda artık birinci ve ikinci fıkra hükümleri değil, dördüncü fıkra hükmü uygulanır…
Faile, dördüncü fıkra uyarınca ceza verildiği hallerde, artık, birinci ve ikinci fıkra uyarınca ceza verilmeyecektir.
Maddenin dördüncü fıkrasının uygulandığı hallerde, suçun banka veya kredi kurumu veya kamu kurum ve kuruluşu aleyhine işlendiğinden bahisle, üçüncü fıkra hükmü uygulanmayacaktır." Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7321.
1210 Apaydın, "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", s. 250; Doğan, a.g.e., s. 152.
1211 İnternet üzerinden başkasının hesabına para aktarılması eylemini TCK' nın 142. maddesinin 2. fıkrasının e bendi kapsamında sayan kararlar için bkz. Yargıtay 6. Ceza Dairesi, 2.6.2008 t., E: 2008/555, K: 2008/12249; Yargıtay 11. Ceza Dairesi, 15.12.2009 t., E: 2008/8714, K: 2009/15828; Yargıtay 11. Ceza Dairesi, 24.12.2009 t., E: 2009/12066, K: 2009/16721; Yargıtay 11. Ceza Dairesi, 13.4.2011 t., E: 2011/723, K: 2011/2028.

Ceza Genel Kurulu'nun aynı konuda eylemin nitelikli hırsızlık oluşturacağına dair 2009 yılında vermiş olduğu kararından sonra Yargıtay Ceza Dairelerinde bu tür olaylarda 142/2-e' nin uygulanacağı görüşü hakim olmuştur.[1212] Yargıtay Ceza Genel Kurulu' nun kararında:

> *"Sanık Volkan'ın; firari Saim ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Ş...bank Ankara K... Şubesindeki hesabından 10.750 YTL'yi Ş...bank-İstanbul Z... Şubesinde sanık Volkan adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir. Kaldı ki sanığın katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCY'nin 142/2-e maddesinde düzenlenmiş bulunan "bilişim sistemi kullanılmak suretiyle hırsızlık" suçunun gerçekleştiği kabul edilmelidir. Şu halde, sanığın eyleminin 5237 sayılı TCY'nin 142/2-e maddesindeki*

İnternet üzerinden başkasının hesabına para aktarılması eylemini TCK' nın 244. maddesinin 4. fıkrası kapsamında sayan kararlar için bkz. Yargıtay 11. Ceza Dairesi, 27.1.2009 t., E: 2008/15441, K: 2009/80; Yargıtay 11. Ceza Dairesi, 27.4.2009 t., E: 2009/964, K: 2009/4877; Yargıtay 11. Ceza Dairesi, 7.10.2009 t., E: 2009/1616, K: 2009/11328; Yargıtay 11. Ceza Dairesi, 22.01.2008 t., E: 2008/8423, K: 2008/117; Yargıtay 11. Ceza Dairesi, 28.02.2008 t., E: 2008/22, K: 2008/1141; Yargıtay 11. Ceza Dairesi, 28.02.2008 t., E: 2008/23, K: 2008/1160, Yargıtay 11. Ceza Dairesi, 26.09.2007 t., E: 2007/5875, K:2007/7637.

1212 Koca ve Üzülmez, a.g.e., s. 836; Akbulut, *Bilişim Alanında Suçlar,* s. 229; Doğan, a.g.e., s. 155, 156; Yılmaz, a.g.e., s. 92.

Yargıtay 8. Ceza Dairesi' nin 3.11.2015 tarihli, E: 2015/5649, K: 2015/23798 sayılı kararında:

"… Akbank Ağrı şubesinde .....personeli olan sanığın, bu bankada döviz hesabı bulunan katılan Y.. T.. adına Akbank Özgür Bankacılık Parola formu düzenlemek suretiyle internet bankacılığı başvurusunda bulunarak, aldığı şifre ile katılanın hesabından, kendi ve başkalarının hesabına para aktarması ve bu parayı kullanması biçiminde gerçekleşen eyleminin, 5237 sayılı TCK.nun 142/2-e maddesinde öngörülen bilişim suretiyle hırsızlık suçunu oluşturduğu gözetilmeden, yazılı biçimde hüküm kurulması, … (BOZULMASINA)" karar verilmiştir. Bkz. https://legalbank.net/arama, ET. 15 Temmuz 2020.

Yine Yargıtay' ın 29.3.2017 tarihli, E: 2016/12069, K: 2017/3405 sayılı kararında: "Şikayetçinin banka hesabına internet bankacılığı aracılığıyla girilerek hakkında hükmün açıklanmasının geri bırakılmasına karar verilen diğer sanığın banka hesabına havale edilmesi eyleminin, TCK.nun 142/2-e madde ve fıkrasında düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden, suç vasfında yanılgıya düşülerek yazılı şekilde TCK.nun 244/4. maddesi uyarınca mahkumiyet hükmü kurulması,… BOZULMASINA" karar verilmiştir. Bkz. https://legalbank.net/arama, ET. 15 Temmuz 2020.

Aynı yönde diğer kararlar için bkz. Yargıtay 8. Ceza Dairesi, 22.11.2017 t., E: 2017/16623, K: 2017/13121; Yargıtay 2. Ceza Dairesi, 16.11.2017 t., E: 2016/12279, K: 2017/11940; Yargıtay 2. Ceza Dairesi, 6.2.2019 t., E: 2019/381, K: 2019/1993.

nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında; 244. maddenin 4. fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır."[1213]

şeklinde gerekçeye yer vermiştir. Koca' nın da belirtmiş olduğu gibi suçun konusunu verinin temsil ettiği ve maddi bir varlığı olan para oluşturmakta olduğundan ve failin kastının yönelmiş olduğu parayı almada bilişim sistemi araç olarak kullanıldığından doktrinde aksi görüşte olan yazarlar[1214] bulunmakta ise de karar isabetlidir.[1215] Dülger' in de belirtmiş olduğu gibi 142/2-e (bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu) düzenlemesinde esas olan verilerin çalınmasından ziyade hırsızlık suçunda bilişim sistemlerinin kullanılması olup paranın veri formuna dönüştüğü ve dijitalleşen dünyada verinin ekonomik bir değeri de olduğu göz önüne alındığında veri formundaki paranın, para olarak bu suça konu olacağının kabulü gerekmektedir.[1216]

Ancak Yargıtay, eski kararlarında rızası dışında kontör transferi yapma şeklinde gerçekleşen eylemi ise 244. m.' nin 4. fıkrası kapsamında değerlendirmekte[1217] iken yeni tarihli vermiş olduğu bir kararda bilgisayar aracılığıyla kontör aktarımı işlemini 142/2-e kapsamında değerlendirmiştir.[1218]

1213 Yargıtay Ceza Genel Kurulu, 17.11.2009 t., E:2009/11-193; K:2009/268, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1214 Özbek, v.d.' ne göre: "Kanımızca bu halde de havale edilen şey bir bilişim sistemi kullanıldığı sürece "veri"dir. TCK m.244 hırsızlık ve dolandırıcılık suçlarına göre bu yönüyle özel bir norm niteliği taşımaktadır. Aynı konuda özel bir norm var iken genel norma gidilemez. TCK m.244'ün getirilmiş amacı bilişim alanında gerçekleşen suç niteliği taşıyan her türlü eylemi cezalandırmaktır. Bu suçlarda ortak payda suçun işlendiği yerin bilişim sistemi olması ve hukuki konunun da "veri" niteliğinde bulunmasıdır…dolayısıyla eylemin veri tarafından temsil edilen paranın mal edilmesine yönelik olduğunu ifade ederek TCK m. 244/4'ün değil TCK m. 142/2-e'de düzenlenen "bilişim sistemi aracılığıyla nitelikli hırsızlık" suçunun gerçekleştiğini kabul ettiği kararına katılamıyoruz." bkz. Özbek, v.d., a.g.e., s. 945, 946.

1215 Koca ve Üzülmez, a.g.e., s. 837.

1216 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 464, 469.

1217 "…Suç tarihinde sanığın internet üzerinden girdiği şifre ile müştekinin GSM numarasından başka bir GSM numarasına, oradan da yine şifre vasıtasıyla kendi numarasına müştekinin bilgisi ve rızası dışında kontör transferi yapma şeklinde gerçekleşen eyleminin TCK'nın 244/4. maddesindeki suçu oluşturduğu gözetilmeden suç vasfında yanılgıya düşülerek yazılı şekilde hüküm kurulması,… BOZULMASINA" bkz. Yargıtay 13. Ceza Dairesi, 30.1.2013 t., E: 2011/26435, K: 2013/1955, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Dülger "Kontör gibi GSM hattına TL yüklenmesi şeklinde gerçekleşen eylemlerde de TCK'nın 142/2-e maddesinin uygulanması gerektiğini" belirtmektedir. Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 470.

1218 "Vodafone şirketine ait kontörleri internet üzerinden ve işyerine ait bilgisayar aracılığıyla ilgili siteler vasıtasıyla transfer ve fatura tahsilatı yapan, bahse konu siteler tarafından giriş kodu ve şifresi verilen katılanın kontör yüklediği siteye girilerek bilgisi dışında, hattına kontör aktarımı yaptığı anlaşılan sanığın eyleminin TCK.nun 142/2-e. maddesinde düzenlenen suçu oluşturacağı gözetilmeden suç vasfında yanılgıya düşerek yazılı şekilde hüküm kurulması,… BOZULMASINA" bkz. Yargıtay 8. Ceza Dairesi, 14.3.2018 t., E: 2017/23361, K: 2018/2812, https://legalbank.net/arama, ET. 15 Temmuz 2020.

Yargıtay Ceza Genel Kurulu, kredisi bitmiş manyetik telefon kartları üzerinde değişiklikler yapılarak görüşme yapan sanık hakkında ise 244. m.' nin 4. fıkrasında yer alan suçun oluştuğuna hükmetmiş ancak çoğunluk görüşüne katılmayan muhalefet şerhinde ise varolan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği ve parasal değer ifade eden 70 adet kontörü alarak mal edinmeye yönelik olduğundan 142/2-e m.' sinde düzenlenmiş bulunan "bilişim sistemi kullanılmak suretiyle hırsızlık" suçunun oluştuğu belirtilmiştir.[1219]

Yargıtay, bir bilişim sistemi olan ATM' lere fiziksel etkide bulunarak içindeki paranın alınması eylemlerinde ise 244. m.' nin 4. fıkrasının uygulanmasına karar vermiştir.[1220]

Günümüzde yaygın olarak internet üzerinden oynanan sanal gerçeklik oyunlarındaki öznelerin 3. kişiler tarafından şifrelerinin kırılması veya hukuka aykırı olarak ele geçirilmesine ilişkin olarak ise Yargıtay yeni tarihli kararlarında 244. m.' nin 4. fıkrasından cezaya hükmetmektedir.[1221]

1219 "…Somut olayda sanığın, kredisi bitmiş olan manyetik telefon kartları üzerinde yaptığı değişikliklerle, sistemin verileri farklı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklenmesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan 765 sayılı Türk Ceza Yasasının 525 b maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu, gerekse suçtan sonra yürürlüğe giren 5237 sayılı Türk Ceza Yasasının 244. maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır. Uygulamada hangi Yasanın daha lehe sonuç verdiği hususu da Yerel Mahkemece değerlendirilip saptanmalıdır. Bu itibarla, Yargıtay Cumhuriyet Başsavcılığı itirazının reddine karar verilmelidir…" Yargıtay Ceza Genel Kurulu, 19.6.2007 t., E: 2007/6-136, K: 2007/150, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1220 'Sanıkların O. bankası ATM'sinin çalışmasındaki aksaklığı fark ederek, çeşitli zamanlarda para çekme işlemi sırasında ATM'ye fiziki müdahalede bulunmak suretiyle cihazın para bloke edilmiş gibi işlem görmesini sağlayıp, çektikleri paranın hesaptan düşmesini engelleyerek menfaat elde ettiklerinin iddia ve kabul olunması karşısında eylemlerinin 765 sayılı TCK'nın 525/b-1 (5237 sayılı TCK'nın 244/4) maddesindeki "bilişim sistemini engellemek veya yanlış biçimde çalışmasını sağlamak suretiyle yarar sağlamak" suçuna uygun bulunduğu gözetilmeden yazılı şekilde 765 sayılı TCK'nın 525/b-2. maddesinden hüküm kurulmak suretiyle eksik ceza tayini… bozmayı gerektirmiştir.' Bkz. 'Yargıtay 11. Ceza Dairesi, 14.3.2012 t., E: 2010/6346, K: 2012/3544' (*Aktaran* Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 348; Yaşar, Gökcan ve Artuç, a.g.e., s. 7334).

1221 "1-Katılanın 23.10.2011 tarihinde ... isimli oyunu oynarken bilgi ve rızası dışında e-posta adresine girilerek şifresinin ve e-posta adresinin değiştirildiğini ve oyun karakterlerinin çalındığını, karakterlerini çalan şahsın olaydan 10 dakika önce kendisine mesaj gönderdiğini, oyun içi iletişim sayesinde çalınan oyun karakterlerini ... isimli şahsın satın aldığını beyan ettiği; dosya kapsamına göre olay günü sanığın babası adına kayıtlı ve fakat sanık tarafından kullanılan IP adresi üzerinden katılanın e-posta adresine erişimin sağlandığı sabit ise de sanığın savunmasında, katılana ait e-posta adresini ... isimli oyunun hilelerinin ve kullanılmayan karakterlerinin paylaşıldığı forum sitesi olan www.onlinehile.org isimli sitede gördüğünü ve sitede bulunan şifre ile giriş yaptığını, oyun karakterlerinin ise sitede bulunmadığını ve suçlamayı kabul etmediğini söylediği; 03.01.2014 tarihli bilirkişi raporunda bilgisayara format atıldığından e-posta adresinin çalınması dışında oyun karakterlerinin çalındığının net olarak tespit edilemediğinin belirtildiğinin anlaşılması karşısında; savunmada belirtilen hususlar da araştırılarak, oyun sitesinden suç tarihinde katılanın kullanıcı adı

Yargıtay, bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu (m. 158/1-f) ile 244/2 ün arasındaki fark için, dolandırıcılık suçunun temel şeklinin oluşması bakımından unsur olan fail tarafından bir insana karşı hileli hareketlerin yapılmasını arayarak bilişim sistemi kullanılarak gerçek kişinin yanıltılarak haksız bir kazanç elde edilmesi halinde 158/1-f nitelikli dolandırıcılık, bir insana yönelik hileli davranışlar sergilenmeksizin sırf bilişim sistemi kullanılarak haksız yarar sağlanması

ve şifresi ile oyuna giriş yapılıp yapılmadığının sorularak, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren ... ve/veya kimin kullanımında olduğunun ve olaydan önce katılana mesaj gönderen kişinin kim olduğunun araştırılarak, yine talimat mahkemesinde beyanı alındığı sırada katılan tarafından dosyaya ibraz edilen CD içeriği ile tüm deliller birlikte değerlendirilip, gerektiğinde bilişim suçlarından anlayan tercihen bilgisayar mühendisi bir bilirkişiden rapor da alınmak suretiyle, toplanan ve toplanacak delillerin birlikte değerlendirilmesi ile sonucuna göre tüm deliller çerçevesinde sanığın hukuksal durumunun tayini gerekirken, bu konularda kovuşturma genişletilmeden eksik inceleme ve yetersiz gerekçe ile yazılı şekilde karar verilmesi,

2-Kabule göre de;

a-Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar sağlanmasının; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği, bu itibarla; suçun sübutu halinde eylemin, 5237 sayılı TCK'nın 244/4. maddesindeki suçu oluşturacağı gözetilmeksizin suç vasfında yanılgıya düşülerek yazılı şekilde hüküm kurulması, … BOZULMASINA" bkz. Yargıtay 13. Ceza Dairesi, 10.10.2017 t., E: 2016/2155, K: 2017/10403, https://legalbank.net/arama, ET. 15 Temmuz 2020. Aynı yönde bkz. Yargıtay 8. Ceza Dairesi, 13.12.2017 t., E: 2017/1283, K: 2017/14186.

Benzer olayda 142/2-e' den hüküm kurulan kararlar için bkz. Yargıtay 8. Ceza Dairesi, 17.2.2016 t., E: 2015/14257, K: 2016/1702; Yargıtay 8. Ceza Dairesi, 22.12.2015 t., E: 2015/7063, K: 2015/26040.

halinde ise 244/4' ün oluşacağı[1222] ölçütünü benimsemiştir.[1223] Yargıtay Ceza Genel Kurulu' nun 2009 tarihli kararından itibaren ise Yargıtay gerçek kişiye karşı aldatıcı

1222 "Somut olayda; sanığın, katılan Mücahit S'in kimlik bilgilerine göre düzenlenip kendi fotoğrafı yapıştırılmış ele geçirilemeyen sahte nüfus cüzdanını kullanarak katılan A A.Ş.nin Yenigün Şubesi'nde hesap açtırarak diğer katılan Murat Ç'ın bankada bulunan para hesabındaki var olan verileri (bilgileri) sahte kimlikle açtırdığı hesaba internet yoluyla havale edip hesap cüzdanı ibraz ederek banka şubesinden çektiğinin iddia ve kabul olunması karşısında; eyleminin, paranın sanığın açtırdığı hesaba intikaline kadar katılan Murat Ç'a yöneltilmiş hile bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle 5237 sayılı TCK. nun 244/4 maddesine uyan suçu oluşturduğu gözetilmeden, vasıflandırılmada yanılgıya düşülerek unsurları oluşmayan banka aracı kılınmak suretiyle nitelikli dolandırıcılık suçundan mahkûmiyet hükmü kurulması, … BOZULMASINA" bkz. Yargıtay 11. Ceza Dairesi, 22.1.2008 t., E: 2007/8423, K: 2008/117; https://legalbank.net/arama, ET. 15 Temmuz 2020.
Aynı yönde diğer kararlar için bkz. Yargıtay 11. Ceza Dairesi, 9.6.2008 t., E: 2008/5591, K: 2008/5863; Bkz. Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 476.
"Somut olayda ise; sanığın, katılanın G... Bankası 1. Levent Şubesi'nde bulunan hesabına internet bankacılığı yoluyla girip hesaptaki paradan 3.200.00 TL'yi G... Bankası Osmanbey Şubesi'ndeki kendi hesabına internet yoluyla havale ettikten sonra parayı çekerek haksız menfaat sağladığı iddia ve dosya içeriğine uygun kabul edilmesi karşısında; gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle dolandırıcılık suçunun unsurlarının bulunmadığı, "veri"nin taşınabilir bir mal olarak kabul edilmesinin olanaklı olmaması nedeniyle hırsızlık suçunun unsurlarının da gerçekleşmediği eylemin, suç tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b (5237 sayılı TCK'nın 244/4. maddesine uygun "bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama" maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden, suçun nitelendirilmesinde yanılgıya düşülerek bilişim sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetine karar verilmesi, … BOZULMASINA" bkz. Yargıtay 11. Ceza Dairesi, 7.10.2009 t., E: 2009/1616, K: 2009/11328, https://legalbank.net/arama, ET. 15 Temmuz 2020.
"…Sanığın, şikayetçilere ait hesaplardan internet aracılığı ile kendi hesabına para aktarmaktan ibaret eyleminde gerçek kişiye yönelik hile ve desise bulunmadığı gözetilmeden 5237 Sayılı TCK. nun 244/4. maddesi yerine suç vasfında hataya düşülerek dolandırıcılık suçundan hüküm kurulması, … BOZULMASINA" bkz. Yargıtay 11. Ceza Dairesi, 18.9.2007 t., E: 2007/6963, K: 2007/5533, https://legalbank.net/arama, ET. 15 Temmuz 2020. "Bu karardan da anlaşılacağı üzere, şayet hile teşkil eden hareketler bir bilişim sistemi aracılığıyla doğrudan bir kişiye karşı gerçekleştiriliyorsa, burada md. 244/4 değil md. 158/1-f çerçevesinde nitelikli dolandırıcılık suçu işlenmiş olacaktır." Bkz. Özbek, v.d., a.g.e., s. 944.
1223 Koca ve Üzülmez, a.g.e., s. 837.
"1-Şikayetçi ile eşinin internet ortamında MSN'de iletişim yaptıkları sırada müştekinin eşine ait elektronik posta adresine ait şifreyi bir şekilde elde edip şikayetçi ile sanki eşiymiş gibi görüşmeye devam ederek onu kandırıp cep telefonu için kontör isteyip şikayetçinin MSN'den gönderdiği kontörleri satmak suretiyle haksız yarar sağlayan sanığın eyleminin bilişim sisteminin araç olarak kullanılması suretiyle 5237 sayılı TCK'nın 158/1-f maddesindeki dolandırıcılık suçunu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi, … BOZULMASINA" bkz. Yargıtay 11. Ceza Dairesi, 18.3.2010 t., E: 2007/5408, K: 2010/3253, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay Ceza Genel Kurulu' nun nitelikli dolandırıcılık suçu için gerekli yasal unsurları açıkladığı bir kararında: "Sanığın,... Varol ismiyle www.....com adlı internet sitesine üç adet dizüstü bilgisayar satışı için ilan verdiği, Gaziantep ilinde yaşayan katılanın internetteki satış ilanını görüp sanığı ilanda belirtilen telefon numarasından aradığı, sanıkla yaptıkları telefon görüşmesi sonucu bilgisayarların 1.500 Lira bedelle satışı konusunda anlaştıkları, sanığın, ortağı olduğunu söylediği tanık ...'in banka hesap numarasını vererek bu hesaba kargo ile gönderdiği bilgisayarların satış bedelini yatırmasını istediği, katılanın verilen hesaba 04.09.2010 tarihinde 1.500 Lira havale ettiği ancak sanığın, tanık....'ün hesabına yatırılan parayı almasına rağmen söz konusu bilgisayarları katılana göndermediği,
Katılanın aşamalarda; www.....com isimli internet sitesinde dizüstü bilgisayar satış ilanı gördüğünü, ilanda belirtilen telefon numarasını aradığını, kendisini... Varol olarak tanıtan sanıkla üç adet bilgisayar için 1.500 Liraya anlaştıklarını, bir süre sonra sanığın kendisini arayarak bilgisayarları kargoya verdiğini ve parayı ortağı ...'e ait banka hesabına yatırmasını istediğini

söylemesi üzerine verilen banka hesabına parayı havale ettiğini, ancak bilgisayarların kendisine gönderilmediğini, tekrar aradığında ise sanığın kendisini oyaladığını, daha sonraki aramalarında da küfredip telefonu kapattığını söylediği,
Tanık ...'in aşamalarda; sanığı, arkadaşı olan tanık ... vasıtası ile tanıdığını, olay tarihinde Zeki ile birlikte evine gelen sanığın, kendisine bir yerden para geleceğini söyleyip, Garanti Bankasında hesabının olup olmadığını sorduğunu, maaşını bu bankadan çektiği için hesabının bulunduğunu söylemesi üzerine hesap numarasını istediğini, bir sakınca görmeyip hesap numarasını verdiğini, daha sonra hesabına yatırılan 1.500 Lirayı bankamatikten çekerek sanığa verdiğini beyan ettiği; tanık ...'ın da aşamalarda benzer ifadelerde bulunduğu,
Sanığın savcılıkta;... Varol ismini kullanmadığını, benzer suçlardan hakkında soruşturmalar olduğunu ancak bu olayın kendisi ile ilgisinin bulunmadığını, ismi geçen tanıkları tanımadığını,
Mahkemede ise; internet üzerinden elektronik eşya satışı yaptığını, 1.500 Lira karşılığında dizüstü bilgisayar satma konusunda katılanla anlaştıklarını, katılanın parayı arkadaşı olan tanık....'ün hesabına yatırdığını,....'ün de parayı çekip kendisine verdiğini, internet üzerinden yapılan satışlarda teslimat için 90 gün ile 180 gün arasında değişen bir süre olduğunu, ancak teslim süresi henüz dolmadan başka suçtan tutuklandığını, bu nedenle katılana bilgisayarı veremediğini savunduğu,
Anlaşılmaktadır.
Uyuşmazlığın sağlıklı bir hukuki çözüme kavuşturulabilmesi için öncelikle "dolandırıcılık" suçunun unsurlarının açıklanmasında yarar bulunmaktadır.
5237 sayılı TCK'nun “Dolandırıcılık” başlıklı 157. maddesi; “Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası verilir” şeklinde düzenlenmiş, suçun daha fazla ceza verilmesini gerektiren nitelikli hallerine ise 158. maddede yer verilmiştir.
Malvarlığının yanında irade özgürlüğünün de korunduğu dolandırıcılık suçunun oluşabilmesi için;
1) Failin bir takım hileli davranışlarda bulunması,
2) Hileli davranışların mağduru aldatabilecek nitelikte olması,
3) Failin hileli davranışlar sonucunda mağdurun veya başkasının aleyhine, kendisi veya başkası lehine haksız bir yarar sağlaması,
Şartlarının birlikte gerçekleşmesi gerekmektedir.
Fail kendisi veya başkasına yarar sağlamak amacıyla bilerek ve isteyerek hileli davranışlar yapmalı, bu davranışlarla bir başkasına zarar vermeli, verilen zarar ile fiil arasında uygun nedensellik bağı bulunmalı ve zarar da, nesnel ölçütler göz önünde bulundurularak belirlenecek ekonomik zarar olmalıdır.
Görüldüğü gibi, dolandırıcılık suçunu malvarlığına karşı işlenen diğer suç tiplerinden farklı kılan husus, aldatma temeline dayanan bir suç olmasıdır. Birden çok hukuki konusu olan bu suç işlenirken, sadece malvarlığı zarar görmemekte, mağdurun veya suçtan zarar görenin iradesi de hileli davranışlarla yanıltılmaktadır. Madde gerekçesinde de, aldatıcı nitelik taşıyan hareketlerle, kişiler arasındaki ilişkilerde var olması gereken iyiniyet ve güvenin bozulduğu, bu suretle kişinin irade serbestisinin etkilendiği ve irade özgürlüğünün ihlâl edildiği vurgulanmıştır.
Bu açıklamalardan sonra uyuşmazlık konusuyla ilgili dolandırıcılık suçunun nitelikli hallerinden olan "bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık" ve "basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle dolandırıcılık" suçlarının üzerinde durulması gerekmektedir.
Bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçu, suç tarihinde yürürlükte bulunan TCK’nun 158/1-f maddesinde; “(1) Dolandırıcılık suçunun;….f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,…İşlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur. Ancak, (e), (f) ve (j) bentlerinde sayılan hâllerde hapis cezasının alt sınırı üç yıldan, adlî para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz” şeklinde düzenlenmiştir.
Madde gerekçesinde de; “Dolandırıcılık suçunun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi de, birinci fıkranın (f) bendinde bu suçun bir nitelikli unsuru olarak kabul edilmiştir. Bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır” açıklamalarına yer verilmiş olup, bu bentte bilişim sistemleri ile banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık olmak üzere birden fazla nitelikli hal kabul edilmiştir.
Türk Dil Kurumu'nun Büyük Türkçe Sözlüğü'nde, “elektronik beyin” veya “bilgileri otomatik işleme tabi tutmuş sistem” olarak adlandırılan bilgisayar; "çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran, bilgileri

depolayan elektronik araç, elektronik beyin" anlamına gelmektedir. İnternet ise, dünya üzerindeki milyonlarca bilgisayarın birbirlerine bağlanmaları ile oluşan global bir bilgisayar ağları sistemini ifade eder. Bilişim de; "insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi" olarak tanımlanmaktadır. Yerleşmiş yargısal kararlar ve öğretideki baskın görüşlere göre de, bilişim sisteminin, verileri toplanıp yerleştirdikten sonra otomatik işleme tabi tutma imkanı veren manyetik sistemler olduğu kabul edilmiştir.

5237 sayılı Türk Ceza Kanununda bilişim suçları; "Bilişim alanında suçlar" bölümünde düzenlenmekle beraber ayrıca, çeşitli bölümlerde de bilişim sistemleriyle işlenmesi mümkün olan suç tiplerine yer verilmistir. "Bilişim alanında suçlar" bölümünde yer alan 243. maddesinde bilişim sistemine girme, 244. maddesinde sistemi engelleme, bozma, verileri yok etme veya değiştirme, 245. maddesinde banka veya kredi kartlarının kötüye kullanılması suçları düzenlenmiştir. Bunun yanında, "Özel hayata ve hayatın gizli alanına karşı suçlar" bölümünde yer alan 135. maddesinde kişisel verilerin kaydedilmesi, 136. maddesinde kişisel verileri hukuka aykırı olarak verme veya ele geçirme, 138. maddesinde ise verilerin yok edilmemesi suçları bilişim suçu olarak nitelendirilebilecek şekilde düzenlenmiştir. Öte yandan, 132. maddesinde haberleşmenin gizliliğini ihlal, 124. maddesinde haberleşmenin engellenmesi, 125/2. maddesinde hakaret, 142/2. maddesinin (e) bendinde hırsızlık, 158/1. maddesinin (f) bendinde dolandırıcılık, 226. maddesinde müstehcenlik, 163. maddesinde karşılıksız yararlanma suç tiplerinin bilişim sistemlerinin kullanılması suretiyle işlenmeleri mümkün kabul edilmiştir.

Günümüzde bilişim sistemleri ile sesli-görüntülü haberleşme, elektronik imzanın kabulü, yeni ticari ilişkiler, internet bankacılığı hizmeti ile para transferleri ve bunlar gibi pek çok yenilik toplumsal hayata girmiş, bilişim gerek iş gerekse günlük hayatta vazgeçilemeyecek kadar önemli bir noktaya ulaşmış, bilişim teknolojileri daha hızlı ve ucuz bir nitelik arz etmesi nedeniyle, klasik yöntemlere nazaran daha fazla tercih edilir duruma gelmiştir. Bu sistemlerin güvenle kullanılması, aynı anda hızlı ve kolayca birçok kişiye ulaşılması ve diğer taraftaki failin kontrol imkanını azaltması nedeniyle nitelikli hal sayılmıştır.

Bilişim sisteminin aldatılmasından söz edilemeyeceği için, ancak bu sistemin araç olarak kullanılarak bir insanın aldatılması yani dolandırılması halinde bu bendin uygulanması mümkündür. Aksi halde yani sisteme girilerek bir kişi aldatılmayıp sistemden yararlanılarak çıkar sağlanmışsa bilişim suçu veya bilişim sistemi kullanılmak suretiyle hırsızlık suçunun oluşması sözkonusu olacaktır.

Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle dolandırıcılık suçu ise TCK'nun 158/1-g maddesinde; "(1) Dolandırıcılık suçunun; ...g) Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle,... İşlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur" şeklinde düzenlenmiştir. Madde gerekçesinde de belirtildiği üzere, dolandırıcılık suçunun basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle işlenmesi bu suç açısından bir nitelikli unsur olarak kabul edilmiştir.

"Basın ve yayın yolu ile" kavramı 5237 sayılı TCK'nun 6. maddesinde;

"(1) Ceza kanunlarının uygulanmasında;

…g) Basın ve yayın yolu ile deyiminden; her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar,

… Anlaşılır" şeklinde tanımlanmıştır.

Madde gerekçesinde de; " 'Basın ve yayın yolu ile' deyimine ilişkin tanım, sadece kitle iletişim araçlarını kapsayacak biçimde değiştirilmiştir. Tasarıdaki bireysel iletişimi de içine alacak şekilde ifade edilmiş olan tanımın oluşturduğu sakıncanın giderilmesi için, tanımda değişiklik yapılarak 'kitle iletişim araçları' ifadesine vurgu yapılmıştır" açıklamalarına yer verilmiştir.

TCK'nun 6/1-g maddesindeki tanıma göre "basın ve yayın yolu ile" deyimi; yazılı, görsel, işitsel ve elektronik her türlü kitle iletişim aracıyla yapılan yayınları içermekte olup, bireysel iletişim araçları bu kapsam dışında bırakılmıştır. Kitle iletişim araçları, kitlesel boyutta ileti dağıtabilen araçlar olup radyo, televizyon, gazete ve internet gibi araçlar en yaygın biçimde kullanılan kitle iletişim araçları arasında yer almaktadır.

Basın ve yayın araçlarının aynı anda bir çok kişiye ulaşması, toplumu yönlendirme ve bireyler arası etkileşimdeki önemli rolü göz önüne alındığında, suçun icrasını kolaylaştırdığı ve eylemin aldatacılık vasfını arttırdığı gözetilerek, dolandırıcılık suçunun basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle işlenmesi nitelikli hal olarak düzenlenmiştir.

Bu nitelikli halin uygulanabilmesi için, basın ve yayın araçlarının kullanılmış olması yeterli değildir. Basın ve yayın araçlarının kullanılmasının suçun işlenmesini kolaylaştırması, hileli hareketlerin

hareketler bulunmadığında olayın özelliklerini dikkate alarak 142/2-e nitelikli hırsızlık suçundan karar vermektedir.[1224]

3.2.3. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçları (TCK madde 245)

Banka veya kredi kartlarının kötüye kullanımın yaptırıma bağlandığı 245. m. :

"(1) 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.

(2) 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.

---

gerçekleştirilmesi ve mağdurun aldatılmasında etkili olması gerekmektedir. Ayrıca suçun işlenmesinde basın ve yayın araçlarının kim tarafından kullanıldığı önemli değildir.
Bu açıklamalar ışığında uyuşmazlık konusu değerlendirildiğinde;
İbrahim Varol ismiyle "www.....com" adlı internet sitesinde dizüstü bilgisayar satışı için ilan veren sanığın, bu ilanı görüp kendisini telefonla arayan katılanla, bilgisayarların 1500 Lira bedelle satışı konusunda anlaşması, bir süre sonra katılanı telefonla arayarak bilgisayarları kargoya verdiğini söyleyip, bedelini vereceği hesap numarasına yatırmasını istemesi üzerine, bildirdiği banka hesabına 1500 Lira yatıran katılana sözde alışverişe konu bilgisayarları göndermemesi şeklinde gerçekleşen olayda; sanığın hem bilişim sistemini araç olarak kullanmak hem de basın ve yayın aracının sağladığı kolaylıktan yararlanmak suretiyle suçu işlediği anlaşıldığından, sanığın bu eylemi ile TCK'nun 158. maddesinin 1. fıkrasının (f) bendinde düzenlenen "bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık" ve aynı fıkranın (g) bendinde düzenlenen "basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle dolandırıcılık" olmak üzere dolandırıcılık suçunun iki farklı nitelikli halininin oluştuğu, bu durumda suçun daha ağır cezayı içeren nitelikli hali olan "bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık" suçundan hüküm kurulması gerektiği kabul edilmelidir…" bkz. Yargıtay Ceza Genel Kurulu, 17.1.2017 t., E: 2015/867, K: 2017/13, https://legalbank.net/arama, ET. 15 Temmuz 2020. Aynı yönde bkz. Yargıtay 15. Ceza Dairesi, 16.4.2015 t., E: 2013/10471, K: 2015/23856.

1224 'Sanık P. A.'nın PTT görevlisinin izni olmadan bilgisayarı kullanarak tanık N.K.'in posta çeki hesabına havale gelmiş gibi işlem yapmak suretiyle 4950 liranın hesap sahibi adına, diğer sanık S. A.'ya teslimini sağladığı, dolandırıcılık suçunun oluşması için gereken kişilere karşı aldatıcı hareketlerde bulunulmayıp bilişim sistemi kullanılmak suretiyle ödemede bulunulmasının sağlandığı; bu nedenle eylemin Ceza Genel Kurulunun 17.11.2009 gün, 177-268 sayılı kararında belirtildiği üzere TCK'nın 142/2-e maddesinde yazılı bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması…' 'Yargıtay 11. Ceza Dairesi, 10.12.2009 t., E: 2007/1260, K: 2009/16657' (*Aktaran* Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 476, 477).
"…1- Katılana ait olan (Z.) Bankası (S.) şubesi nezdindeki internet şubesi hesabına sanığın, haksız yere elde ettiği katılana ait şifre ile girerek, 2.080 TL parayı yeğeni olan tanık (S.M.)'a yatırdığı, 24.04.2006 günü ise 6.577 TL parayı kendi hesabına aktardığının anlaşılması karşısında, sanığın eylemi 5237 sayılı TCK'nın 142/2-e maddesindeki suçu oluşturduğu halde aynı Yasanın 158/1-f.maddesi ile uygulama yapılması, … BOZULMASINA" bkz. Yargıtay 13. Ceza Dairesi, 11.6.2013 t., E: 2013/3821, K: 2013/17985, https://legalbank.net/arama, ET. 15 Temmuz 2020.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır. ”[1225]

şeklinde düzenlenmiştir.

Banka veya kredi kartlarının kötüye kullanımına ilişkin 5237 sayılı TCK' nın 245. m.' sinde yer alan bu düzenlemenin 765 sayılı eski TCK' da karşılığı olan bir madde bulunmamaktaydı.[1226] Uygulamada sıklıkla karşılaşılan bu fiiller ise somut olayın özelliklerine göre 525b. m.' sinin 2. fıkrasında yer alan bilişim sistemi marifetiyle yarar sağlama, bazen de kartların ele geçiriliş şekillerine göre hırsızlık, dolandırıcılık, güveni kötüye kullanma suçları kapsamında cezalandırılıyordu.[1227] Ancak, 765 sayılı TCK' nın 525 b/2 m.' sinde yer alan bilgileri otomatik işleme tabi tutan sistem kullanılarak hukuka aykırı yarar elde edilmesi suçunun banka veya kredi kartlarının kullanılmasıyla hukuka aykırı yarar elde edilmesi fiilini kapsayıp kapsamadığı doktrinde tartışılan bir konuyu oluşturmuş ve Yargıtay Ceza Genel Kurulu 2001 yılında vermiş olduğu karar ile bahse konu eylemlerin 765 sayılı TCK' nın 525 b/2 m.' si kapsamında olduğunu belirtmiştir.[1228] Yargıtay Ceza Genel Kurulu'

1225 https://mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf, ET. 25 Mart 2020.

1226 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6970.

1227 Koca ve Üzülmez, a.g.e., s. 843.

"Uyuşmazlık konusu olan olaylardan birinde Yargıtay 6. CD yerel mahkemenin kararını, "Müştekiye ait kredi kartını ele geçiren sanığın, bu kartı kullanarak iki gün ara ile ATM'den para çekmekten ibaret eyleminin, kredi kartının alet olarak kullanılması karşısında, TCK'nın 493/2, 80. maddelerindeki suçu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek aynı yasanın 525/b-2. maddesi ile uygulama yapılması" gerekçesiyle bozmuştur…Diğer bir olayda ise, yine aynı daire benzer bir fiili dolandırıcılık olarak nitelendirmiştir. Bu karara göre, "özel bankalarca düzenlenen kartların henüz sahiplerine teslim edilmeden çalınıp kullanılması eylemi bankaya yönelik olup TCK'nın 503/1 ve 80. maddesinde yazılı suçu" oluşturmaktadır." Bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 270.

1228 'YCGK 10.04.2001 T. ve 2001/76-30 E:2001/757 K-: 'Y… Bankası'nın Çiftehavuzlar şubesindeki ATM'nin, kart konulan bölümüne önceden kağıt yerleştiren sanığın, işlem yapmak isteyen şikayetçinin kartının sıkışmasını sağlayıp, böylece sistemle iletişimi ve işleme geçilmesini engellediği, yardımcı olmak bahanesiyle önceden anlaştığı arkadaşını cep telefonu ile arayarak

nun bu kararından sonra bankamatik kartlarıyla ilgili olaylarda 525/b-2 m.' si uygulanmışsa da[1229] bu kez banka veya kredi kartının ele geçiriliş ve kullanılışına göre bilgileri otomatik işleme tabi tutan sistem kullanılarak hukuka aykırı yarar sağlama suçunun mu yoksa dolandırıcılık suçunun mu oluştuğu hususu tartışılmıştır.[1230] 5237 sayılı TCK, bu tartışmaların son bulması, duraksamaların ve içtihat farklılıklarının önlenmesi veya ortadan kalkması adına banka veya kredi kartlarının kötüye kullanımı fiillerini bağımsız bir suç haline getirmiştir.[1231]

245. m.' nin gerekçesi ise:

"Madde, banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme alınmıştır.

Banka kartı, bankanın kurduğu sisteme hukuka uygun olarak girmeyi sağlamaktadır. Bu kart, saptanan ve kart sahibince bilinen bir numara marifetiyle, banka görevlisinin yardımı olmadan, kart sahibinin kendi hesabından para çekmesini sağlamaktadır.

Kredi kartları ise, banka ile kendisine kart verilen kişi arasında yapılmış bir sözleşme gereğince, kişinin bankanın belirli koşullarla sağladığı kredi olanağını kullanmasını sağlayan araçtır.

İşte bu kartların kötüye kullanılmaları, söz konusu maddede suç olarak tanımlanmıştır. Maddeye göre, aşağıdaki şekillerde gerçekleştirilen hareketler bu suçu oluşturmaktadır:

1. Başkasına ait bir banka veya kredi kartının, her ne suretle olursa olsun ele geçirilmesinden sonra, sahibinin rızası bulunmaksızın kullanılması veya kullandırttırılması ve bu suretle failin kendisine veya başkasına haksız yarar sağlaması.

2. Aynı fiilin, aynı koşullarla sahibine verilmesi gereken bir banka veya kredi kartının bunu elinde bulunduran kimse tarafından kullanılması veya kullandırttırılması; söz

---

şikayetçi ile görüşmesini sağladığı, kartını geri alabilmek, olmazsa kartın kullanımını iptal ettirebilmek umuduyla görüşen şikayetçiye banka görevlisi gibi davranan arkadaşının şifre kodlama işlemi sırasında şikayetçinin şifresini öğrendiği, onun ayrılmasından sonra da kredi kartını yuvadan çıkartıp Y. Bankası'nın anlaşmalı olduğu P.'nin iki ayrı şubesindeki ATM'den farklı tarihlerde toplam 600 milyon TL nakit kredi çektiği dosyadaki belge ve kanıtlardan anlaşılmaktadır. Yukarıdaki açıklamalar ışığında somut olay değerlendirildiğinde, sanığın haksız olarak ele geçirdiği bir başkasına ait kart ve şifreyi kullanarak bir bankanın iki farklı şubesindeki ATM makinesinden para çekip hukuka aykırı yarar sağlaması eylemi TCY'nin 493/2. madde ve fıkrasındaki suçu değil aynı yasanın 525/b.2 madde ve fıkrasında düzenlenen bilgileri otomatik isleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu oluşturduğundan Yargıtay C. Başsavcılığı'nın itirazının kabulüne karar verilmelidir.' (*Aktaran* Doğan, a.g.e., s. 157, 158, dipnot. 536)

1229 Akbulut, *Bilişim Alanında Suçlar*, s. 271.

1230 Doğan, a.g.e., s. 158; Akbulut, *Bilişim Alanında Suçlar*, s. 271.

1231 Yaşar, Gökcan ve Artuç, a.g.e., s. 7337.

gelimi kartı sahibine vermekle görevli banka memurunun kartı kendi veya başkası yararına kullanması.

Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis'lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirilmeleri uygun görülmüştür.

Maddenin ikinci fıkrasına göre; birinci fıkrada belirtilen fiillerin, oluşturulmuş sahte bir banka veya kredi kartını kullanmak suretiyle işlenmesi, daha ağır ceza ile cezalandırılmayı gerektirmektedir. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir."[1232]

TCK'nın 245. m.' si, Kanun' un yürürlüğe girdiği tarih olan 1.6.2005 tarihinden itibaren iki kez değişikliğe uğramış, bunlardan ilki, maddeye 2. ve 4. eklenmesini içeren 29.6.2005 tarihli ve 5377 sayılı Kanunla gerçekleştirilen değişiklik olup ikincisi ise maddeye 5. fıkranın eklenmesini içeren 6.12.2006 tarihli ve 5560 sayılı Kanun ile gerçekleştirilen değişikliktir.[1233]

245. m.' nin ilk 3 fıkrasında 3 farklı suç düzenlenmişse de biz suçla korunan hukuksal yarar başlığı altında da belirteceğimiz ve esasen madde gerekçesinde de belirtilmiş olunduğu üzere 245. m. düzenlemesinin aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının banka veya kredi kartlarının kullanılarak işlendiği şekilleri olarak bağımsız ve kendine özgü bir norm olarak düzenlenmiş hali olarak kabul ettiğimiz[1234] ve 245. m. düzenlemesinin tümü itibariyle öncelikli olarak malvarlığı değerlerini koruduğunu düşündüğümüzden malvarlığına karşı suçlar bölümünde düzenlenmesinin daha uygun olacağını değerlendirmekteyiz.[1235] Madde metninde düzenlenen suç tiplerinin koruduğu

1232 A.e., s. 7335, 7336.

1233 Ayrıntılı bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 275; Koca ve Üzülmez, a.g.e., s. 843; Yaşar, Gökcan ve Artuç, a.g.e., s. 7337.

1234 Aynı yönde bkz. Kurt, a.g.e., s. 179; Koca ve Üzülmez, a.g.e., s. 845.

1235 Aynı yönde bkz. Koca ve Üzülmez, a.g.e., s. 846, 847. Koca ve Üzülmez, 245. madde düzenlemesinin topluma karşı suçlar kısmının bilişim alanında suçlar bölümünde yer verilmesinin sebebini: "Diğer taraftan, bu suçla, ticari hayatta nakit para yerine yaygın bir şekilde kullanılan banka ve kredi kartlarının kötüye kullanılması da önlenmek istenmiştir. Özellikle kredi kartlarıyla yapılan alışverişlerin kişinin kendisine ait gerçek bir kartla yapıldığına yönelik toplumda oluşan güvenin korunması gerekir Aksi takdirde başkası adına düzenlenmiş gerçek veya sahte kartların alışverişlerde kullanılmasının yaygınlaşması halinde, bu kartlara olan talep azalacak ve bu durum bankacılık sisteminin ve ekonomik yapının sağlıklı bir şekilde işleyişi bakımından ciddi problemler ortaya çıkartacak, kayıt dışı ekonomik faaliyetlerin artmasına yol açacaktır. Kanun koyucu banka ve kredi kartlarının ticari hayatta gördüğü bu fonksiyon nedeniyle olsa gerek, bu suça kanunun malvarlığına karşı suçlar bölümünde değil, topluma karşı suçlar kısmının bilişim alanında suçlar bölümünde yer vermiştir." şeklinde açıklamaktadır. Bkz. A.e., s. 846.

"Hal böyle olunca suçla korunan hukuki yararı ortaya koyarken yararlanılabilecek ve sistematik yorum yöntemi olarak da ifade edilen suçun düzenlendiği yer anlamsızlaşmaktadır. Gerçekten bu

hukuksal değerin malvarlığı değerleri olarak ortak olması sebebiyle de suçun unsurları, aynı başlık içerisinde ancak suç tiplerinin birbirlerinden farklılaştığı noktalara değinilmek suretiyle incelenecektir.

3.2.3.1. Korunan Hukuksal Değer

TCK' nın 245. m.' sinde birden fazla suç yer almakta olup kanun koyucu madde gerekçesinde maddenin "banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme" alındığını bunun yanında"hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis'lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla" bağımsız bir suç düzenlendiğini belirtmiştir.

Kanaatimizce, bu suç ile korunmak istenen hukuksal değer karma nitelikte[1236] olup öncelikle hırsızlık, dolandırıcılık, güveni kötüye kullanma fiillerini içermesi

---

suç TCK'nın Đkinci Kitabının Topluma Karşı Suçlar başlıklı Üçüncü Kısmının Bilişim Alanında Suçlar başlıklı Onuncu Bölümünde düzenlenmektedir. Böylece bir yandan söz konusu suçun "topluma karşı" bir suç olduğu kabul edilirken, diğer yandan "bilişim suçu" olduğu da kabul edilmiş olmaktadır. Bu durumda korunan hukuki yararın kamu güveni ve bilişim alanı olduğu söylenebilir. Ancak hem madde içeriği hem de gerekçesi, hükmün bilişim alanı ile doğrudan bir ilgisi olmadığını ortaya koymaktadır. Bu yönüyle hükmün düzenlendiği yerin gözden geçirilmesinin yerinde olacağı söylenebilir. Ancak söz konusu suçun/suçların temel özelliğinin bu suç ya da suçların bilişim sistemine karşı ya da bilişim sistemi araç kılınmak suretiyle işlendiği ifade edilmelidir. Bu suç/suçların esasen bilişim alanı vasıta kılınmak suretiyle işlendiği söylenmelidir…" bkz. Veli Özer Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 9, Özel Sayı, 2007, ss. 1019-1063, s. 1022.

"…bu suç her ne kadar bilişim alanında suçlar başlığı altında yer alsa da daha çok malvarlığına karşı işlenen suç izlenimi vermektedir…

…Hal böyle olunca suçlar korunan hukuki değerin ortaya koyarken yararlanılabilecek ve sistematik yorum yöntemi olarak da ifade edilen suçun düzenlendiği yer anlamsızlaşmaktadır. Gerçekten bu suç TCK'nın İkinci Kitabının Topluma Karşı Suçlar başlıklı Üçüncü Kısmının Bilişim Alanında Suçlar başlıklı Onuncu Bölümünde düzenlenmektedir. Böylece bir yandan söz konusu suçun "topluma karşı" bir suç olduğu kabul edilirken, diğer yandan "bilişim suçu" olduğu da kabul edilmiş olmaktadır. Bu durumda korunan hukuki değerin kamu güveni ve bilişim alanı olduğu söylenebilir. Ancak hem madde içeriği hem de gerekçesi, hükmün bilişim alanı ile doğrudan bir ilgisi olmadığını ortaya koymaktadır. Bu yönüyle hükmün düzenlendiği yerin gözden geçirilmesinin yerinde olacağı söylenebilir…" bkz. Özbek, v.d., a.g.e., s. 951. Özbek, v.d., 245. madde düzenlemesinin topluma karşı suçlar kısmının bilişim alanında suçlar bölümünde yer verilmesinin sebebini: "…Sonuç olarak, m.245'te düzenlenen suç ile korunan hukuki yarar karma bir nitelik arz etmekte bilişim sistemi ile işlendiğinden yasakoyucunun suçun/suçların düzenleniş yeri itibariyle tercihini bilişim alanı olarak kullandığı söylenmelidir." şeklinde açıklamıştır. Bkz. A.e., s. 952.

Aksi görüşte olan Taşkın' a göre ise: "TCK 245. maddesinin; eski yasadaki karşılığı olan TCK 525/b.2'deki düzenleme ve bu düzenlemeyi açıklığa kavuşturan yukarıda tarih ve sayısı belirtilen Yargıtay CGK kararı ile birlikte değerlendirildiğinde ve maddenin gerekçesi de gözetildiğinde bilişim alanındaki suçlar bölümünde düzenlenmesinin doğru olduğu kanısını taşıyoruz." Bkz. Taşkın, a.g.e., s.59.

1236 Suçun karma nitelik taşıdığını belirten Doğan' a göre ise: "…bu kartlarla madde kapsamına giren suçlar işlendiğinde kamunun bu bilişim sistemlerine olan güveni zedelenecek, kart kullanımı azalacak, bu durum ise hem ticari yaşamın ve hem de bankacılık sisteminin olumsuz etkilenmesine

sebebiyle öncelikle malvarlığı, güveni kötüye kullanma suçu açısından kişilerin birbirlerine karşı duyduğu güven ve sahtecilik suçunu karşılaması açısından ise kamuya duyulan güven ve itibardır.[1237] Ancak banka ve kredi kartlarının kötüye kullanılması da önlenmek istendiğinden madde düzenlemesinin dolayısıyla bilişim sisteminin sağlıklı ve güvenli işleyişinin de korunmak istendiği söylenebilecektir.[1238] Ancak Koca' nın da belirtmiş olduğu gibi kişinin malvarlığının zarara uğratılmasında veya sahtecilik suçu açısından bakıldığında ise sahteciliğin gerçekleştirilmesinde banka veya kredi kartı ve bu kartların kullanıldığı bilişim sistemi sadece bir araç fonksiyonu gördüğünden[1239] bu suçun bilişim sistemi olmaksızın işlenememesi ve bilişim sistemleri aracılığıyla çalışan banka ve kredi kartlarıyla ilgili olması suçun bilişim alanında suçlar bölümünde düzenlenmesinin isabetli olduğunu da göstermeye yeterli değildir.[1240] Zira, ilgili başlık altında belirtmiş olduğumuz üzere dar anlamda bilişim suçlarını, koruduğu öncelikli hukuki değeri verilerin ve/veya bilişim sistemlerinin işleyişi ve güvenliğine ilişkin eylemlerin oluşturduğu suçlar, geniş anlamda bilişim suçlarının ise klasik suç tiplerinin işlenişinde bilişim araç, cihaz ve aygıtlarının araç olarak olarak kullanıldığı ancak ihlal edilen öncelikli hukuki değerin ilgili başka suçlara ait olduğu suçlar olarak tanımlamak gerekmektedir. Kaldı ki

---

neden olacaktır. Bu düzlemde hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarıyla korunmak istenen hukuki yararlar TCK 245. madde ile de korunmaktadır. Hırsızlık suçuyla kişilerin malvarlığı, güveni kötüye kullanma suçuyla kişilerin birbirine karşı duyduğu güven, sahtecilik suçuyla devlet tarafından verilen güvence ile belgelere olan güven korunmak istenmiştir." Bkz. Doğan, a.g.e., s. 162.

1237 Aynı yönde bkz. Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345,* s. 6971; Yaşar, Gökcan ve Artuç, a.g.e., s. 7337; Mahmutoğlu, a.g.e., s. 871; Parlar ve Hatipoğlu, a.g.e., s. 3767; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 357.

Dülger' e göre: "245. maddenin 2. fıkrasında ise haksız bir yarar elde edilmesi aranmaksızın yalnızca sahte banka ve/veya kredi kartı üretilmesi, dağıtılması suç haline getirilmiştir. Buna göre suç tipiyle malvarlığının dışında ayrıca ve özellikle bankacılık hizmetlerinin güvenle ve hızlı bir şekilde yapılması, dolayısıyla ekonomik yapının sağlıklı işlemesi güvence altına alınmaktadır…" bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 358.

1238 Yaşar, Gökcan ve Artuç, a.g.e., s. 7338.

"…Ancak hem madde içeriği hem de gerekçesi, hükmün bilişim alanı ile doğrudan bir ilgisi olmadığını ortaya koymaktadır." Bkz. Özbek, v.d., a.g.e., s. 951.

1239 Özbek, v.d.' ne göre de, "Bu suç/suçların esasen bilişim alanı vasıta kılınmak suretiyle işlendiği söylenmelidir." Bkz. A.e., s. 951, 952.

Ancak Kurt: "Banka veya kredi kartı kullanmak suretiyle işlenen bu suç, bir bilişim sistemi olmaksızın işlenememesi nedeniyle bir bilişim suçudur." şeklinde açıklama yaptıktan sonra "Banka ya da kredi kartının verdiği yetkiyle bilişim sistemine girerek hesaptan para çekme ya da diğer bankacılık işlemlerinin yapılması netice itibariyle banka veya kredi kartının sahibinin hesabındaki parası üzerinde gerçekleştirilmektedir. Mağdur olanın malvarlığına yönelik bir eylem söz konusudur." ifadelerini eklemektedir. Bkz. Kurt, a.g.e., s. 178.

1240 Koca ve Üzülmez, a.g.e., s. 846.

"…245. maddenin 1. fıkrasının "bilişim alanında suçlar" bölümünde düzenlenmesiyle, suçla korunan hukuki değer değil hukuki değerin ihlalinde kullanılan araç göz önünde bulundurulmuştur. Bu itibarla böyle bir suç tipi düzenlenecek idiyse, buna malvarlığına karşı suçlar bölümünde yer verilmesi daha yerinde olurdu." Bkz. A.e., s. 846, 847.

Yargıtay Ceza Genel Kurulu 2010 yılında vermiş olduğu bir kararında[1241], başkasına ait kredi kartı ile sahibinin rızası hilafına para çekilmesi eyleminin "malvarlığına karşı işlenen suçların özel bir şekli" olduğunu belirtmek suretiyle söz konusu suç ile korunan hukuksal değerin malvarlığı olduğunu kabul etmiştir.[1242] O halde madde düzenlemesinde bilişim sistemlerinin araç olarak kullanıldığı dolayısıyla suçun koruduğu esas hukuksal değerin malvarlığı değeri olduğu dikkate alındığında madde düzenlemesinin yerinin isabetli olmadığını değerlendirmekteyiz.[1243]

3.2.3.2. Maddi Unsur

3.2.1.3.1. Fail ve Mağdur

245. m.' de düzenlenen suçların faili olabilmek için bir özellik aranmadığından herkes bu suçun faili olabilecektir.[1244] TCK' nın 246. m.' sine göre ise, suçun işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında ise bunlara özgü güvenlik tedbirlerine hükmolunacaktır.[1245]

1241 "…Öğretide benimsenen görüşler ışığında; somut olayımızda olduğu gibi başkasına ait kredi kartı ile sahibinin rızası hilafına para çekilmesinden ibaret eylemin aynı zamanda mal varlığına karşı işlenen suçların özel bir şekli olduğu konusunda duraksama bulunmadığını kabul etmek gerekmektedir…" bkz. Yargıtay Ceza Genel Kurulu, 30.3.2010 t., E: 2010/11-17, K: 2010/65, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yine Yargıtay' ın 25.5.2016 tarihli kararında kısmen karşı oy düşüncesinde de: "…Kısaca belirtmek gerekirse, banka veya kredi kartlarının kötüye kullanılması (TCK m. 245), dolandırıcılık (TCK m. 157, 158) ve belgede sahtecilik (TCK m. 204 vd.) suçları birbirinden ayrı, bağımsız suçlar olup, anılan her bir suçun unsurları ve suçla korunan hukuki yararlar farklıdır. Banka veya kredi kartlarının kötüye kullanılması ile dolandırıcılık suçlarında korunan hukuki yarar banka veya kişilerin malvarlığı iken, sahtecilik suçlarında korunmak istenen hukuksal yararın, belgelerin gerçekliğine ilişkin toplumda oluşan kamu güveni olduğu öğreti ve uygulamada kabul edilmektedir…" hususlarına yer vermilmiştir. Bkz. Yargıtay 8. Ceza Dairesi, 25.5.2016 t., E: 2016/3489, K: 2016/6784, https://legalbank.net/arama, ET. 15 Temmuz 2020.
1242 Koca ve Üzülmez, a.g.e., s. 846; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 358.
1243 Aynı görüşte olan Dülger' e göre de: "…TCK'da bilişim suçları düzenlenirken ETCK'ya getirilen önemli bir eleştiri göz önünde bulundurulmuş ve suçlar düzenlenirken ETCK'ya getirilen önemli bir eleştiri göz önünde bulundurulmuş ve suçlar korudukları hukuksal değere göre ilgili oldukları bölümde diğer suç tipleriyle birlikte düzenlenmiştir; yalnızca koruduğu hukuksal değer karma nitelik gösteren ya da bilişim sistemlerine ve/veya verilere karşı işlenen suç tiplerine aynı bölümde "bilişim alanında suçlar" başlığı altında yer verilmiştir. Ancak, banka veya kredi kartlarının kötüye kullanılması suçlarının koruduğu hukuksal değer bireyin malvarlığı olmasına rağmen bu suçlar malvarlığına karşı suçlar bölümünde değil, bilişim alanında suçlar bölümünde düzenlenmiştir. Bu düzenleme şekli ise yasanın sistematiğine aykırı olduğu için değiştirilmeli ve bu suçlar "malvarlığına karşı suçlar" bölümünde düzenlenmelidir…
…Ceza hukuku tarafından korunan hukuksal değer, yalnızca suç tipinin oluşturulması açısından bir hareket noktası olmayıp, aynı zamanda ceza yasalarının özel kısımlarının sistemleştirilmesi için de bir bağlantı noktasıdır, dolayısıyla ceza yasalarının özel kısmındaki suç tipleri korudukları hukuksal değere göre düzenlenmektedir." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 358, 359.
1244 Koca ve Üzülmez, a.g.e., s. 847; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 360; Yaşar, Gökcan ve Artuç, a.g.e., s. 7338; Parlar ve Hatipoğlu, a.g.e., s. 3767.
1245 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6977; Mahmutoğlu, a.g.e., s. 871; Yaşar, Gökcan ve Artuç, a.g.e., s. 7338.

Mağdur bakımından öncelikle incelenmesi gereken husus 245. m. düzenlemesinde yer alan "kart sahibi" ve "kartın kendisine verilmesi gereken kişi" kavramlarıdır. Zira m.' nin birinci fıkrasında belirtilen kişilerin rızası halinde suç oluşmayacaktır. Doktrinde, "kart sahibi" ifadesinden karta zilyet olma şeklinde anlaşılmaması gerektiği, sırf uygulamadan ortaya çıkan sorunlar sebebiyle madde metnine dahil edilen "kartın kendisine verilmesi gereken kişi" ifadesi olmasa dahi adına banka kartı düzenlenen kişinin kartın sahibi olması sebebiyle bunu da kapsadığı belirtildiği[1246] gibi kartın asıl sahibinin banka veya finans kuruluşu olduğunu belirten yazarlar[1247] da bulunmaktadır.

23.2.2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu' nda (BKKK), kartlı sistem kuruluşu, kart çıkaran kuruluş ve kart hamili ifadeleri tanımlanmıştır.[1248] Buna göre kanaatimizce, doktrinde de belirtildiği üzere madde metninde düzenlenen "kart sahibi" ifadesinden kartın yararlanıcısı konumunda olan kart hamilini anlamak gerekmektedir.[1249] Zira, bu suçla korunan hukuksal değerin malvarlığı olduğu göz önüne alındığında suçun mağdurunun da suçun konusunu oluşturan yararın ait olduğu kişi bir başka deyişle suç nedeniyle malvarlığında azalma

1246 Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 201; Koca ve Üzülmez, a.g.e., s. 848.

1247 Özbek, v.d., a.g.e., s. 958; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 362.

1248 "…f) Kartlı sistem kuruluşu: Banka kartı veya kredi kartı sistemi kuran ve bu sisteme göre kart çıkarma veya üye işyeri anlaşması yapma yetkisi veren kuruluşları,
g) Kart çıkaran kuruluş: Banka kartı veya kredi kartı düzenleme yetkisini haiz bankalar ile diğer kuruluşları,…
…j) Kart hamili: Banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişiyi, … ifade eder." şeklinde tanımlanmıştır.

1249 Aynı yönde bkz. Özbek, v.d., a.g.e., s. 958; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 362; Koca ve Üzülmez, a.g.e., s. 848; Yaşar, Gökcan ve Artuç, a.g.e., s. 7339; Akbulut, *Bilişim Alanında Suçlar,* s. 281.
"Banka kartı veya kredi kartları, düzenleme yetkisini haiz bankalar ile diğer kuruluşlar tarafından çıkarılmaktadır. Bankalar ve bu kuruluşlar kartın mülkiyetine sahiptirler. Kart hamilleri ise karttan yararlanma, kartı kullanım hakkına sahip kişilerdir…Banka veya kredi kartlarının kullanılması veya kullandırılması suretiyle çıkar sağlandığında, hesabında azalma veya borç gözüken banka veya kredi kart hamili kullanımdan zarar gördüğünden suçun mağduru kart hamili olacaktır." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 281, 282.
"…Kart hamilliği ise, kartın fiziksel olarak kullanıcıya zilyetliğinin devri ile değil, bu kişi adına kartın üretilmesi ve hesabıyla ilişkilendirilmesiyle gerçekleşir. Dolayısıyla kartın kendisine verilmesi gereken kişi, henüz zilyetlik kendisine devredilmeden de önce kartın hamilidir ve dolayısıyla bu suçun da mağdurudur." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 362.
"5464 sayılı Kanundaki tanım esas alındığında TCK'daki "kart sahibi" ifadesinin doğru olmadığı söylenebilir. Zira kart hamili kartın sahibi değil, yararlanıcısıdır. Esasen kartın asıl sahibi banka ya da finans kuruluşudur. Dolayısıyla TCK'da yer alan kart sahibi ibaresini kart hamili olarak anlamak gerektiği düşüncesindeyiz. Yine "kartın kendisine verilmesi gereken kişi" de esasen kart hamilidir. Sonuç olarak TCK'daki tereddüte yol açabilecek olan bu ifadeler yerine "kart hamili" teriminin kullanılması daha doğru olacak ve mevzuatta birlik de sağlanmış bulunacaktır." Bkz. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1030.

olan kişi olarak kabul etmek gerekir.[1250] Bu noktada, kartı çıkaran bankanın suçun mağduru olup olmadığı hususunda doktrinde fikir birliği bulunmamaktadır. Suçun mağdurunun kartın hamili gerçek veya tüzel kişi, bunun yanında banka veya kredi kartının asıl sahibi durumunda bulunan banka veya finans kurumu olduğunu belirten yazarlar[1251] bulunduğu gibi suçun mağdurunun malvarlığında azalma meydana gelen gerçek kişi olduğu bankanın ise suçtan zarar gören olarak kabul edilmesi gerektiğini belirten yazarlar[1252] da bulunmaktadır. Yargıtay' ın ise somut olayın özelliklerine göre (kartın teslim edilip edilmemiş olması ayrımına giderek) mağduru tespit ettiği kararları[1253] bulunmakla birlikte Yargıtay Ceza Genel Kurulu' nun 2011 yılında vermiş olduğu kararda da belirtildiği üzere "suçun mağduru kredi veya banka kartı hamili" olup "suçun işlenmesinde her ne kadar banka ve kredi kurumunun bilişim sistemi aracı olarak kullanılmakta ve banka kartlarının mülkiyeti bankaya ait ise de; bu hususlar suçun mağduru olduğu anlamına gelmemekte, bu durumda banka veya kredi kurumları 'suçtan zarar gören' konumundadır".[1254]

1250 Koca ve Üzülmez, a.g.e., s. 847; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 365.

1251 Özbek, v.d., a.g.e., s. 956, 957; Parlar ve Hatipoğlu, a.g.e., s. 3767.
Yaşar, Gökcan ve Atruç' a göre: "…Birinci fıkrada düzenlenen banka ve kredi kartının kötüye kullanılması suçunun mağduru, kural olarak kredi veya banka kartı olan herkes olabilir. Yani burada mağdur, kural olarak kart hamilidir. Kart hamilinin gerçek kişi olması ile, tüzel kişi olması arasında fark yoktur…" bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7339.

1252 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6977; Mahmutoğlu, a.g.e., s. 871; Akbulut, *Bilişim Alanında Suçlar*, s. 284; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 364-366.
"…bu suç nedeniyle malvarlığında azalma olan kişi suçun mağdurudur. Ancak eylem gerçekleştirilirken fail tarafından, mağdurun üzerinde hakimiyeti olmayan ve kendisinin malvarlığına dahil olmayan banka veya finans kurumunun bilişim sistemi, otomatik para çekme makinesi ve kredi veya banka kartı kullanılmaktadır. Bu araçların kullanılmasıyla her ne kadar banka veya finans kurumunun malvarlığında bir azalma dolayısıyla zarar söz konusu olmamaktaysa da; oluşan suç ile bu kurumların bilişim sistemlerinin ve kartlarının güvenilirliği ile genel olarak ticari itibarları zarar görmektedir. Bu nedenle söz konusu bu kurumlar bu suç tipinde "suçtan zarar gören" konumundadır…" bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 365.

1253 "…tüm eylemler değerlendirildiğinde, kredi kartı almak için yapılan başvuruların sanıklar tarafından yapılmayıp gerçek kişiler tarafından bizzat yapıldığı ancak sahiplerine teslim edilmemesi halinde mağdur banka olup TCK.nun 245/1, 43., kart teslim edilmiş ancak hukuka aykırı şekilde gerek fiziki gerekse kart bilgilerinin ele geçmesi suretiyle kullanılmaları halinde ise mağdur adına kart düzenlenen kişiler olup mağdur sayısınca aynı yasanın 245/1. maddesindeki suç oluşacağı,…" bkz. Yargıtay 8. Ceza Dairesi, 27.6.2016 t., E: 2016/1579, K: 2016/8464, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Ancak Yargıtay 8. Ceza Dairesi' nin vermiş olduğu bir kararda da bankanın suçtan zarar görmediği belirtilmiştir: "…TCK.nun 245/1. maddesinde düzenlenen banka veya kredi kartının kötüye kullanılması suçunun mağduru kart sahibi olup, suçtan doğrudan zarar görmeyen Türkiye İş Bankası'nın davaya katılma hakkı bulunmadığı halde, katılan sıfatı ile davaya kabulüne karar verilip…" bkz. Yargıtay 8. Ceza Dairesi, 31.5.2017 t., E: 2016/10951, K: 2017/6370, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1254 "…Mağdur; Türk Dil Kurumu Büyük Türkçe Sözlüğünde, "haksızlığa uğramış kişi" olarak tanımlanmaktadır.
Ceza hukukunda ise mağdur kavramı, suçun konusunun ait olduğu kişi ya da kişilerdir. 5237 sayılı Türk Ceza Yasasının hazırlanmasında esas alınan suç teorisinde suçun maddi unsurları arasında yer

245. m.' nin 2. ve 3. fıkralarında, birinci fıkradan farklı olarak sahte banka veya kredi kartı olması aranmakta olup 2. fıkrada yer alan suç için suçun mağduru için banka hesap sahibi bunun yanında banka veya kredi kartını çıkarma yetkisine sahip banka veya kredi kurumu olduğunu belirten yazarların[1255] yanında özel bir sahtecilik suçu niteliğinde olan 2. fıkrada yer alan mağdurunun toplumu oluşturan herkes olduğunu belirten yazarlar[1256] bulunmakla birlikte Yargıtay' ın bu durumlarda kartın henüz kullanılmaması sebebiyle bankanın mağdur sıfatına haiz olacağı yönünde vermiş olduğu kararları bulunmaktadır.[1257] 3. fıkra içinse burada tümüyle sahte, hayali hesaplara bağlı olarak üretilen kartlar söz konusu olduğundan bu suçun mağdurunun banka ya da finans kurumu olduğunu belirten yazarlar[1258] olduğu gibi kendisine ait kartta sahtecilik yapılıp kullanılan kartın hamili ile birlikte bankanın suçun mağduru olduğunu belirten yazarlar[1259] da bulunmaktadır. Yargıtay ise, sahte banka veya kredi

---

alan mağdur, ancak bir gerçek kişi olabilecek, tüzel kişilerin suçtan zarar görmeleri olanaklı ise de bunlar mağdur olamayacaklardır. Suçtan zarar gören ile mağdur kavramları da aynı şeyi ifade etmemektedir. Mağdur suçun işlenmesiyle her zaman zarar görmekte ise de suçtan zarar gören kişi her zaman suçun mağduru olmayabilir. Bazı suçlarda mağdur belirli bir kişi olmayıp; toplumu oluşturan herkes (geniş anlamda mağdur) olabilecektir…
TCY'nın 245/1. maddesinde düzenlenen suçun mağduru kredi veya banka kartı hamilidir. Ayrıca birinci fıkrada; "kartın kendisine verilmesi gereken kişi"den söz edilmekte olup, bu kişi de esasen kart hamilidir. Suçun işlenmesinde her ne kadar banka ve kredi kurumunun bilişim sistemi aracı olarak kullanılmakta ve banka kartlarının mülkiyeti bankaya ait ise de; bu hususlar suçun mağduru olduğu anlamına gelmemekte, bu durumda banka veya kredi kurumları "suçtan zarar gören" konumundadır…" bkz. Yargıtay Ceza Genel Kurulu, 18.10.2011 t., E: 2011/6-166, K: 2011/213, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1255 Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1046.

1256 Koca ve Üzülmez, a.g.e., s. 863; Akbulut, *Bilişim Alanında Suçlar*, s. 314.
"…Her ne kadar sahte banka veya kredi kartının başkalarının hesaplarıyla ilişkilendirilerek üretilmesi gerekiyor ise de bu suçun oluşması bakımından kartın kullanılması gerekmediği için hesap sahibinin veya bankanın fiilin işlenmesiyle zarar görmesi mümkün değildir. Esasında bu suç böyle bir mağduriyetin oluşmasını engellemek için ihdas edilmiştir." Bkz. Koca ve Üzülmez, a.g.e., s. 863.

1257 "…5237 sayılı TCK. nun 245/2. maddesinde tanımlanan suçun mağdurunun, kartın henüz kullanılmamış olması nedeniyle hesap sahibi olmayıp banka veya kredi kartını çıkarma yetkisine haiz banka olacağı ve Bankalar Arası Kart Merkezi'nin 07.02.2008 günlü yazısında suça konu kopyalanmış kartların Amerikan Express-United states ve EURO Kartensysteme Gmbh adlı iki ayrı bankaya ait olduğunun tesbit edilmesi karşısında sanığın eyleminin teselsül eden iki ayrı suç oluşturduğu gözetilmeden yazılı şekilde tek suçtan hüküm kurulması…" bkz. Yargıtay 11. Ceza Dairesi, 9.4.2009 t., E: 2009/630, K: 2009/4067, https://legalbank.net/arama, ET. 15 Temmuz 2020. Aynı yönde bkz. Yargıtay 11. Ceza Dairesi, 20.2.2008 t., E: 2007/8458, K: 2008/915.
Özbek vd.' ne göre de diğer iki suçtan farklı olarak burada kart henüz kullanılmış olmadığından suçun mağduru banka veya finans kurumudur. Bkz. Özbek, v.d., a.g.e., s. 972.
"…Olayda üretilen ve kullanılan sahte kredi kartlarının aynı bankaya ait olduğu anlaşılmakla; suç mağdurunun kredi kartı üretilen ve kullanılan "banka" olacağı, aynı bankaya ait üretilmiş kartların farklı kişiler adına olması ve bu kartlarla birden fazla işyerinde alışveriş yapılması durumjunda da "zincirleme suç" hükmünün değerlendirilmesi gerekeceği…" bkz. Yargıtay 8. Ceza Dairesi, 7.6.2017 t., E: 2016/10091, K: 2017/6652, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1258 Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1053.

1259 Yaşar, Gökcan ve Artuç, a.g.e., s. 7339.

kartı üretme, kabul etme ve bu kartlar ile para çekme veya alışveriş yapma eylemlerinin mağdurunu banka veya kredi kuruluşu olarak belirlemektedir.[1260]

Kanaatimizce, 1. ve 3. fıkrada yer alan suçlar bir zarar suçu olup hareketlerin neticesinde hasız bir yarar sağlanması neticesi arandığından bu suçların mağduru, malvarlığında azalma meydana gelen gerçek kişiler olup tüzel kişilerin mağdur sıfatına haiz olamayacağı görüşüne katıldığımızdan dolayı da bankanın suçtan zarar gören olarak kabul edilmesi gerektiğini değerlendirmekteyiz. Sahtecilik suçlarında esasen kamuya güven korunduğundan bir görüşte belirtildiği gibi 2. fıkra açıından mağdur, toplumu oluşturan herkes olarak kabul edilebilecekse de 2. fıkrada yer alan suç ise bir nevi özel sahtecilik suçu[1261] niteliği taşıdığından ve fıkrada sahte kart üretme, kabul etme, devretme, kullanma fiillerinin başkalarına ait banka hesaplarıyla ilişkilendirilmesi şartına bağlandığından bu fıkrada yer alan suç açısından mağdurunun esasen kendisine ait olan banka hesabı sahte kart ile ilişkilendirilen gerçek kişi olarak kabul etmek gerektiği değerlendirilmektedir.

3.2.1.3.2. Suçun Konusu

Kanaatimizce 245. m.' nin 1. ve 3. fıkralarında düzenlenmiş olan suçların konusu, banka veya kredi kartı kullanılmak suretiyle sağlanan yarar,[1262] 2. fıkrada düzenlenen suçun hukuki konusunu ise sahte bir şekilde oluşturulan banka veya kredi

---

Koca' ya göre ise "…failin sağladığı yarar nedeniyle malvarlığı zarara uğrayan kişi bu suçun mağdurudur." Bkz. Koca ve Üzülmez, a.g.e., s. 868. Aynı yönde Akbulut, *Bilişim Alanında Suçlar*, s. 332.

1260 "…Sahte banka veya kredi kartı üretme, kabul etme ve sahte oluşturulmuş banka veya kredi kartı ile ATM cihazından para çekme ya da alış veriş yapma eylemlerinin mağduru kredi ya da banka kartını üreten banka veya finans kuruluşu olması nedeniyle, kartı çıkaran banka sayısınca ve aynı bankaya ait birden fazla sahte kart kullanılması halinde ise, kendi içerisinde zincirleme şekilde TCK'nin 245/2. ve 245/3. madde ve fıkralarında düzenlenen suçların oluşacağı cihetle;…" bkz. Yargıtay 8. Ceza Dairesi, 12.5.2015 t., E: 2014/29393, K: 2015/17026, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1261 Soyaslan, a.g.e., s. 663, 664; Akbulut, *Bilişim Alanında Suçlar*, s. 312.
"…m.245/2 ve 3'de düzenlenen suçların kendine özgü bir sahtecilik suçu olduğu söylenmelidir." Bkz. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1046.

1262 Doktrinde bu suçların konusunu banka veya kredi kartı olduğunu belirten yazarlar için bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7339; Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1025; Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, s. 209.
Dülger' e göre ise, 1. ve 3. fıkrada düzenlenen suçlarda hukuka aykırı yararın elde edilebilmesi ancak bir banka veya kredi kartıyla gerçekleştirilebileceğinden ve bu kartlar suçun üzerinde işlendiği bilişim sisteminin bir parçası olduğundan 1. ve 3. fıkrada yer alan suçların konusunu sağlanan yarar yanında banka veya kredi kartları da oluşturmaktadır. Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 369.

kartı oluşturmaktadır.[1263] Zira, suçla korunan hukuksal yarar başlığında da belirtmiş olduğumuz üzere, yapılan düzenleme ile öncelikle hırsızlık, dolandırıcılık, güveni kötüye kullanma fiillerini içermesi sebebiyle öncelikle malvarlığı, sahtecilik suçunu karşılaması açısından ise kamuya duyulan güven ve itibar korunmaktadır. 2. fıkrada yer alan suç "özel sahtecilik suçu" niteliğinde fiiller içermekte olup bu suç soyut tehlike suçu niteliği taşımaktadır.[1264]

5464 sayılı Banka Kartları ve Kredi Kartları Kanunu' nda banka kartı[1265]; "Mevduat hesabı veya özel carî hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kart", kredi kartı ise *"Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarası"* şeklinde tanımlanmıştır.

3.2.1.3.3. Fiil

3.2.1.3.3.1. Başkasına Ait Banka veya Kredi Kartıyla Hukuka Aykırı Yarar Sağlama (245/1)

245. m.' nin birinci fıkrasında yaptırıma bağlanan fiil, failin, başkasına ait bir banka veya kredi kartını, kart sahibinin veya kartın verilmesi gereken kimsenin rızası olmaksızın kullanmak veya başkasına kullandırmak suretiyle kendisine veya başkasına yarar sağlamasıdır.[1266] Bu suçun gerçekleşebilmesi için öncelikle failin söz konusu kartları ele geçirmiş veya elinde bulunduruyor olması gerekmekte olup[1267] kartın hamilin rızası ile veya rızası dışında ele geçirilmiş olunması arasında fark bulunmadığı[1268] gibi fiziken veya bilgilerin ele geçirilmesi arasında fark

1263 Aynı yönde bkz. Koca ve Üzülmez, a.g.e., s. 849, 863, 868; Akbulut, *Bilişim Alanında Suçlar*, s. 284, 314, 333.
1264 Akbulut, *Bilişim Alanında Suçlar*, s. 312.
1265 "Banka kartında mülkiyet, kartı çıkaran bankaya ait olmakta müşteriye (hamile) sadece kullanım hakkı verilmektedir. Banka kartının ön yüzünde ait olduğu kurumun ayırıcı işaretleri, kullanıcının adı soyadı, kart numarası ve kartın geçerlik süresi bulunmakta; kartın arka yüzünde ise kart ve kulanıcısına ait bilgilerin sayısal veri halinde bulunduğu manyetik şerit yer almaktadır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 367; Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1027.
"…kredi kartının banka kartından farklı olarak "basılı kart veya fizikî varlığı bulunmayan kart numarası" şeklinde tanımlandığına dikkat çekilmelidir. Bu durum m.245/1'de yer alan suçun işlenmesi bakımından bu suçun konusunu oluşturan kartın fiziksel olarak kullanılması gerektiği yönündeki düşünceyi dayanaksız bırakmaktadır." Bkz. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1028.
1266 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6971, 6972.
1267 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 371; Parlar ve Hatipoğlu, a.g.e., s. 3768; Mahmutoğlu, a.g.e., s. 872.
1268 Bkz. Yargıtay 11. Ceza Dairesi, 19.2.2009 t., E: 2008/8392, K: 2009/1235, www.kazanci.com›kho2/ibb/giris.html, ET. 15 Temmuz 2020.

bulunmamaktadır.[1269] Yargıtay 8. Ceza Dairesi, bir kararında, "para çekmek için bankamatik kartını ATM cihazına yerleştiren ve şifresini giren katılanla sohbet eden sanığın gizlice ATM cihazının para çekme tuşuna basıp katılan uzaklaştıktan sonra çekilen tutarı alması şeklinde gelişen" eylemde sanığın kredi kartını ya da kart bilgilerini ele geçirmemiş olmasını gözeterek TCK' nın 141. m.' sinde yer alan hırsızlık suçunun oluştuğuna karar vermiştir.[1270] Yine Yargıtay bir başka kararında ise

1269 Yaşar, Gökcan ve Artuç, a.g.e., s. 7343; Parlar ve Hatipoğlu, a.g.e., s. 3768; Mahmutoğlu, a.g.e., s. 872.
"…Söz konusu kartların ve bu kartlara ait şifrelerin kullanılması sonucu internet üzerinden girilen banka hesabından ya da kartlar kullanılarak yapılan alışverişler neticesinde hukuka aykırı yarar elde edilmesi halinde de suç oluşmaktadır." Bkz. Soyaslan, a.g.e., s. 658.
"Kartın kullanılması suretiyle hesaptan para çekmek veya kredi kartlarıyla alışveriş yaparak yarar sağlamak durumunda banka veya kredi kartının kötüye kullanılması suçu söz konusu olmaktadır. Kartın kullanılmasında ise mutlaka fiziken kartın ele geçirilmesi, elde bulundurulması, kartın ATM'ye sanık tarafından takılması, şifrenin sanık tarafından girilmesi zorunluluğu bulunmamaktadır. Önemli olan kart üzerinde tasarrufta bulunularak yarar sağlanılmasıdır. Maddedeki "her ne surette olursa olsun" tabiri bu fikri desteklediği gibi, kredi kartı bilgileri kullanılarak mail-order yöntemiyle yapılan alışverişlerde banka ve kredi kartının kötüye kullanılması suçunun oluşması da-ki uygulamada bu konuda tereddür bulunmamaktadır-kartın fiziken elde bulundurulması zorunluluğunun olmadığının en önemli kanıtıdır. Zaten kart olmadan sanığın yarar sağlaması mümkün değildir. Önemli olan yararın kart aracılığı ile elde edilmesidir. Kartın katılan tarafından ATM'ye takılmasının, şifrenin katılan tarafından girilmesinin, kartla sanığın fiziken temasta bulunup bulunmamasının bir önemi yoktur… " bkz. Yargıtay 8. Ceza Dairesi, 16.6.2016 tarihli, E: 2016/5303, K: 2016/8057, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yargıtay 11. Ceza Dairesi'nin bir kararında: "Oluşa uygun kabule göre, bir şekilde elde ettiği mağdura ait kredi kartı bilgilerini kullanarak cep telefonuna kontör yüklemek ve internet üzerinden alışveriş yapmak suretiyle haksız yarar sağlamak şeklinde gerçekleşen olayda; 5464 Sayılı Banka Kartları ve Kredi Kartları Kanununun 3/e maddesi uyarınca "kredi kartının, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını" ifade etmesi karşısında; eylemin T.C.K.nun 245/1. maddesinde tanımlanan "banka ve kredi kartlarının kötüye kullanılması" suçunu oluşturacağı, mağdura ait kredi kartının sahtesi üretilerek kullanıldığına dair herhangi bir tespit ve delil de bulunmadığı gözetilmeden, suç vasfında yanılgı sonucu T.C.K.nun 245/3. maddesinin uygulanması suretiyle yazılı şekilde fazla ceza tayini,…BOZULMASINA" karar verilmiştir. Bkz. Yargıtay 11. Ceza Dairesi, 4.6.2013 tarihli, E: 2012/2220, K: 2013/9277, https://legalbank.net/arama, ET. 15 Temmuz 2020.
1270 Bkz. Yargıtay 8. Ceza Dairesi, 17.6.2015 t., E: 2014/37160, K: 2015/19397, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Ancak Akbulut' un da haklı olarak belirttiği üzere bu olayda TCK madde 244/2 çerçevesinde gerçekleştirilen bir fiille çıkar sağlanması söz konusu olduğundan 244/4 ün uygulanması gerekmektedir. Bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 292.
Yargıtay 8. Dairesi aynı yönde vermiş olduğu bir başka kararında:
"Şikayetçinin para çekmek için gittiği ATM'de kartıyla işlem yapmak üzere şifresini girdiği, para çekme bölümüne sanığın yerleştirdiği düzenek nedeniyle para ve kartını alamadığı, bankanın kapalı olması ve orada bulunan yardım bahanesiyle yaklaşan sanıkla beraber şikayetçinin şifreyi tekrar girip yine işlem yapamaması üzerine oradan uzaklaşması sonucu sanığın ATM'den çıkan parayı alıp uzaklaştığı, şikayetçinin daha sonra kartını banka görevlilerinden teslin aldığı anlaşılmakla; sanığın, şikayetçinin kartını alıp kullanmaya yönelik hareketi bulunmayıp hedefinin sadece ATM'deki paraya yönelik olduğu, menkul mal niteliğinde olan paranın zilyedinin rızası dışında alıkonulması nede- niyle eylemin hırsızlık suçunu oluşturacağı gözetilmeden, uygulama alanı bulunmayan TCK.nun 245/1. madde ve fıkrasında tanımlanan banka veya kredi kartlarının kötüye kullanılması suçundan mahkumiyetine hükmedilmesi,…(BOZULMASINA)" Bkz. Yargıtay 8. Ceza Dairesi, 8.4.2015 tarihli, E: 2014/33365, K: 2015/15858, https://legalbank.net/arama, ET. 15 Temmuz 2020.

"akaryakıt istasyonunda kullanılan ve bir şekilde kredi kart bilgileri ele geçirilen kredi kartları ile sahiplerinin izni olmaksızın alışveriş yapılmış gibi slip çektikleri" olayın TCK' nın 245. m.' sinin 1. fıkrası uyarınca cezalandırılması gerektiğinden bahisle bozma kararı vermiştir.[1271] Doktrinde kartın rıza dışında ele geçirilmesi halinde bunun başka bir suçu oluşturması halinde failin ayrıca bu suçtan cezalandırılacağı belirtilmekte[1272] olup Yargıtay da bu görüştedir.[1273] Bunun yanında, failin ele geçirmiş olduğu veya elinde bulundurduğu banka veya kredi kartını mağdurun rızası dışında kullanması gerekmekte olup suç tipinde açıkça yer alan rıza, suçun kurucu unsurunu oluşturmaktadır.[1274] Suç tipinde açıkça yer almış olan rızanın varlığı, bu suç bakımından bir hukuka uygunluk sebebi değil, tipikliği ortadan kaldıran bir hal olarak değerlendirilecektir. Diğer bir deyişle rıza, burada olduğu gibi, hukuka uygunluk sebepleri içinde değil maddi unsur, tipe uygunluk içinde incelenmelidir. Tüm bu sebeplerle kart sahibi tarafından bu suçun işlenebilmesi mümkün değildir.[1275] Bir başka husus da, doktrinde bu suçun icra hareketlerinin "kullanma" veya "kullandırma"

Dülger' e göre de bu olaylarda, "…ATM cihazlarının bir bütün halinde bilişim sistemi oldukları, hatta bankalara ait bilişim sisteminin bir parçası oldukları tartışmasızdır. Dolayısıyla fiziksel bir etkiyle de olsa bunların çalışmasının engellenmesi ve bu engelleme neticesinde haksız yarar elde edilmesi TCK'nın 244. maddesinin 4. fıkrası kapsamına girer. Fail kart kullanmaksızın ancak bilişim sistemine fiziksel etkide bulunmak suretiyle haksız yarar sağladığı için bu fıkra gereğince cezalandırılmalıdır." Bkz. *Dülger, Bilişim Suçları ve İnternet İletişim Hukuku,* s. 383.

1271 "…Dolandırıcılık suçunda unsur olan aldatıcı hareketlerin gerçek kişiye yönelmesi ve gerçek kişinin hataya düşürülerek kendi veya bir başkasının mal varlığı aleyhine, sanık veya bir başkasının lehine bir işlemde bulunmaya yöneltilmesi ve bu işlem sonucunda sanığın kendine veya başkalarının yararına haksız bir menfaar sağlanması gerekir. Somut olayda; sanığın katılan bankaya üye işyeri olarak başvurup pos cihazı aldığı, fikir ve eylem birliği içinde oldukları anlaşılan B… akaryakıt istasyonunda kullanılan ve bir şekilde kredi kart bilgileri ele geçirilen kredi kartları ile sahiplerinin izni olmaksızın alışveriş yapılmış gibi sliğ çektiklerinin anlaşılması karşısında, dolandırıcılık suçunun hile unsurunun oluşmadığı, eylemin suç tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b-2 maddesinde yazılı bilişim sistemini kullanarak yarar sağlama suçunu oluşturacağı gözetilmeden yazılı şekilde hüküm kurulması,… (BOZULMASINA)" bkz. Yargıtay 11. Ceza Dairesi, 22.6.2010 tarihli, E: 2008/11089, K: 2010/7131, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1272 Yaşar, Gökcan ve Artuç, a.g.e., s. 7344.

"…Öte yandan kart hileli davranışlar ile elde edilmiş ise bu hareket bakımından dolandırıcılık mevcut iken, bu şekilde ele geçirilmiş kartın kullanılması halinde ise m.245/1'de yer alan suç oluşur. Kanımızca bu halde TCK m.158/1 f'deki suç oluşmaz. Nihayet bu şekilde elde edilen bir kartın sahte olarak üretilmesi ve daha sonra bu kartın kullanılması mümkündür. Bu halde hem dolandırıcılık, hem de m.245/2 ve 3'de yer alan suçların ayrı ayrı oluştuğu söylenmelidir." Bkz. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1044.

1273 "TCK.nun 245/1. maddesinde "…her ne suretle olursa olsun…" diyerek yasa koyucu, kartın ele geçirilme şeklinin bu suçun oluşumu bakımından önemli olmadığını, hukuka aykırı ele geçirmelerde ise, ayrıca o suçtan da cezalandırılabileceğini ifade etmek için kullanmıştır. O halde sanık, mağdurun kartını yağma veya hırsızlık suretiyle ele geçirebileceği gibi bu suçları işlemeden de kartı elde etmiş olabilir…" bkz. Yargıtay 8. Ceza Dairesi, 7.3.2016 tarihli, E: 2015/15640, K: 2016/2735, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1274 Yaşar, Gökcan ve Artuç, a.g.e., s. 7345.

1275 Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1033.

ile başladığı, ele geçirme ile ilgili hareketlerin suçun icra hareketi olarak nitelendirilemeyeceği, bu sebeple kullandırma veya kullanmaya yönelik hareketler gerçekleştirilmedikçe suçun teşebbüs aşamasına gelmiş olmayacağının belirtilmesidir.[1276]

İkinci olarak suçun oluşabilmesi için failin başkasına ait banka veya kredi kartını kullanma veya kullandırtması gerekmektedir.[1277] Kullanma veya kullandırmanın fiziki varlığından yararlanılarak kullanılıp kullanılmayacağı hususunda doktrinde farklı görüşler[1278] bulunmakta ise de kanaatimizce Yargıtay' ın da kabul etmiş olduğu üzere[1279] failin kartı fiziken veya kart üzerindeki bilgilerini

1276 Bkz. Yaşar, Gökcan ve Artuç, a.g.e., s. 7346; Koca ve Üzülmez, a.g.e., s. 851, 852.
Aynı yönde bkz. Yargıtay 11. Ceza Dairesi, 6.5.2013 t., E: 2012/831, K: 2013/7273.

1277 Soyaslan, a.g.e., s. 659.

1278 Koca ve Üzülmez' e göre; "…O halde banka veya kredi kartlarının kullanılması, bu kartların fiziki olarak ATM ve POS cihazı gibi makinelerden geçirilmesini gerektirmektedir. Bu suç ancak banka veya kredi kartlarının bilişim sistemleri üzerinden kullanılmasıyla işlenebilir. Bu nedenle, kartın fiziki olarak kullanılmayıp karta ilişkin bilgilerin elde edilerek bilişim sistemi yoluyla haksız yarar sağlanması halinde bu suç oluşmaz. Kanaatimizce, bu durumda, somut olayın işleniş şekline göre bilişim sistemini kullanarak hırsızlık, dolandırıcılık veya bilişim sistemlerini kullanarak haksız yarar sağlama (m. 244/4) suçlarına ilişkin hükümler uygulanmalıdır." Bkz. Koca ve Üzülmez, a.g.e., s. 853. Aynı yönde görüş için Erdoğan, *Türk Ceza Kanunu' nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* s. 327.
Özbek' e göre: "Bu suçun oluşması için kartın "fiziksel olarak" kullanılması zorunludur kanısındayız. Hükümde yer alan "kartın kullanılması ya da kullandırılması" sadece karta ilişkin bilgilerin değil, bizatihi kartın kullanılması şeklinde anlaşılmalıdır. Ancak kredi kartının banka kartından farklı olarak "basılı kart veya fiziki varlığı bulunmayan kart numarası" şeklinde tanımlanması karşısında bu suç bakımından kredi kartının fiziksel olarak kullanılmasının zorunlu olmadığı sonucu çıkmaktadır." Bkz. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1032.
Özbek v.d.' ne göre de: "Bu suçun oluşması için kartın "fiziksel olarak" kullanılması zorunludur kanısındayız. Hükümde yer alan "kartın kullanılması ya da kullandırılması" sadece karta ilişkin bilgilerin değil, bizatihi kartın kullanılması şeklinde anlaşılmalıdır.
Bununla birlikte internetin yaygınlaşması bankacılık hizmetlerinin internet üzerinden de verilmesi ve bu suretle internet bankacılığı olarak adlandırılan hizmetlerden ya da internet üzerinden sunulan alışveriş hizmetlerinden yararlanılması sırasında banka ya da kredi kartı üzerindeki bilgilerin ve şifrenin kullanılması mümkündür. Böylece kart bizatihi kullanılmadan sadece üzerindeki bilgilerden yararlanılarak kartın kullanılması ya da kullandırılması olanaklı hale gelmektedir. Bu halde söz konusu bilgilerin sahibinin rızası olmaksızın kullanılması halinde kanımızca m.244/2 ve 3 düşünülmelidir." Bkz. Özbek, v.d., a.g.e., s. 959, 960.

1279 5237 sayılı TCK'nın 245/1. Madde ve fıkrasında, başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimsenin kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa cezalandırılacağı hükme bağlanmıştır. Madde gerekçesinde de belirtildiği üzere; söz konusu madde, "banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi veya banka kartı sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme alınmıştır … Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis'lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç haline getirilmeleri uygun görülmüştür."
Öte yandan 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 3/e maddesine göre kredi kartı, "nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını" ifade etmektedir.

kullanmak suretiyle yarar elde etme arasında fark bulunmamaktadır.[1280] Zira, korunan hukuksal yarar başlığı altında da belirtmiş olduğumuz üzere, burada korunan hukuksal yarar banka veya kredi kartları kullanılmış olmak suretiyle yarar sağlanmasıdır dolayısıyla burada elde edilen yararın kartların fiziken ya da bilgilerinin girilmesi suretiyle kullanılması arasında bir fark bulunmamakta önemli olan bu suretle başka bir deyişle bu kartların bir şekilde kullanılması sonucunda yararın sağlanmasıdır. Bunun yanında, fıkrada açıkça belirtildiği gibi failin kartı kendisinin kullanması ya da başkasına kullandırtması, suçun oluşumu bakımından bir farkı bulunmamaktadır.

Üçüncü olarak ise yukarıda belirtilen eylemler sonucunda haksız bir yararın elde edilmiş olunması gerekmektedir, aksi takdirde kartın kullanımı ya da kullandırılması sonucunda yarar elde edilmedikçe suç tamamlanmış olmayacaktır.[1281] Failin, banka veya kredi kartını kullanmasının sonucunda kendisine veya başkasına sağladığı haksız yarardan, maddi ve ekonomik bir yararı anlamak gerekir.[1282] Zira, malvarlığına ilişkin hakkın korunmakta olduğu bu suç tipinin madde gerekçesinde de açıkça "maddenin banka veya kredi kartlarının hukuka aykırı olarak kullanılması

Somut olayda; müdahili telefonla arayıp bir bankadan aradığını ve banka görevlisi olduğunu, kredi kartından çekilen kart ücretinin iadesi için kart bilgilerinin gerektiğini söyleyen ve müdahilden bu şekilde temin ettiği kart numarası, son kullanma tarihi ve güvenlik numarası bilgilerini mail order sistemiyle kullanarak bir mağazadan alışveriş yapan sanığın eyleminin bir bütün olarak banka ve kredi kartlarının kötüye kullanılması suçunu oluşturduğu gözetilerek 5237 sayılı TCK'nın 245/1. madde ve fıkrası uyarınca cezalandırılması ile yetinilmesi gerekirken yazılı şekilde iki ayrı suç olarak kabulüyle ayrıca dolandırıcılık suçundan da hüküm kurulması yasaya aykırı olup, hüküm bu nedenle bozulması gerekmektedir…" bkz. Yargıtay 8. Ceza Dairesi, 13.6.2012 tarih, E: 2012/11116, K: 2012/20386, https://legalbank.net/arama, ET. 15 Temmuz 2020. Aynı yönde bkz. Yargıtay 11. Ceza Dairesi, 17.9.2008 tarihli, E: 2008/12914, K: 2008/8887; Yargıtay 11. Ceza Dairesi, 3.6.2009 tarihli, E: 2009/4463, K: 2009/6825; Yargıtay 11. Ceza Dairesi, 27.4.2009 tarihli, E: 2006/7564, K: 2009/4868; Yargıtay 8. Ceza Dairesi, 5.5.2014 tarihli, E: 2013/6328, K: 2014/11449.
Yargıtay' ın 2016 tarihli bir kararına da: "Sanığın ele geçirdiği katılana ait kredi kartı bilgilerini (mail order yöntemiyle) kullanmak suretiyle yarar sağlamatan ibaret eyleminin, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 3/e maddesi uyarınca 1kredi kartının, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını" ifade etmesi karşısında; eylemin TCK'nın 245/1. maddesinde tanımlanan "banka ve kredi kartlarının kötüye kullanılması" suçunu oluşturduğu, gözetilmeden suç vasfında yanılgıya düşerek yazılı şekilde hüküm kurulması,…BOZULMASINA" bkz. Yargıtay 17. Ceza Dairesi, 14.3.2016 tarihli, E: 2015/8866, K:2016/3316, https://legalbank.net/arama, ET. 15 Temmuz 2020.

1280 Aynı yönde bkz. Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, s. 298, 299; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 377; Kurt, a.g.e., s. 185; Akbulut, *Bilişim Alanında Suçlar*, s. 284, 294.

1281 Akbulut, *Bilişim Alanında Suçlar*, s. 294.
"Bu suç bakımından netice failin kendisine veya bir başkasına yarar sağlamasıdır. Diğer bir deyişle, suç failin kendisine veya bir başkasına yarar sağlaması ile tamamlanır. Kart kullanılmış ancak yarar sağlanmamış ise suçun teşebbüs aşamasında kaldığı söylenmelidir." Bkz. Özbek, v.d., a.g.e., s. 961.

1282 Koca ve Üzülmez, a.g.e., s. 853; Yaşar, Gökcan ve Artuç, a.g.e., s. 7346.
Akbulut' a göre de ekonomik nitelikte olmayan yararlar bu fıkra kapsamında yer alan suça girmeyecektir. Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 295.

suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek amacıyla kaleme alındığı" belirtilmiştir.

Son olarak belirtmek gerekir ki madde metninde banka veya kredi kartının kullanımına ilişkin bir sınırlama bulunmadığından bu suç serbest hareketli bir suçtur.[1283]

3.2.1.3.3.2. Başkalarına Ait Banka Hesaplarıyla İlişkilendirilerek Sahte Banka veya Kredi Kartı Üretilmesi, Satılması, Devredilmesi, Satın Alınması veya Kabul Edilmesi (245/2)

245. m.' nin 2. fıkrasında, başkalarına ait banka hesabıyla ilişkilendirilerek sahte kart üretmek, kartın sahte olduğunu bilerek satmak, devretmek, satın almak veya kabul etmek fiilleri düzenlenmiş olup söz konusu suç seçimlik hareketli bir suç olmasının yanında seçimlik hareketlerin yapılması ile tamamlandığından aynı zamanda sırf hareket suçudur.[1284] Zira bu suçun oluşması için yarar elde etme şeklinde bir netice gerekmediği[1285] gibi sahte kart üretmenin toplumda bir zarara veya zarar tehlikesine yol açması şartı da aranmadığından söz konusu suç aynı zamanda soyut tehlike suçu niteliği taşımaktadır.[1286]

Sahte bir kartın üretilmesi, başkalarının hesaplarıyla ilişkilendirerek sahte bir kartı meydana getirmek, oluşturmak anlamına gelmekte[1287] olup sahte bir kartı bedel karşılığında başkasına veren "satan", sahte üretilmiş bir kartı bir bedel karşılığında olmaksızın başkasına veren "devreden" ve bu kartı alan da "kabul eden" olarak ifade

1283 Yaşar, Gökcan ve Artuç, a.g.e., s. 7347; Özbek, v.d., a.g.e., s. 961.
1284 Koca ve Üzülmez, a.g.e., s. 863, 864; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 386; Yaşar, Gökcan ve Artuç, a.g.e., s. 7347; Özbek, v.d., a.g.e., s. 973.
Özbek suçun seçimlik hareketli olduğunu belirtmekle birlikte suç tipinde ayrıca netice belirtilmediği, bu yönüyle suçun neticesi harekete bitişik olduğunu ve icrai bir hareketle işleneceğini de belirtmektedir. Bkz. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1048. Aynı yönde bkz. Özbek, v.d., a.g.e., s. 973.
1285 Parlar ve Hatipoğlu, a.g.e., s. 3769.
"…Özellikle çok yaygın şekilde işlenen kredi kartlarının numaralarının ve hesap bilgilerinin ele geçirilerek, bunların sahtesinin yapılması ve diğer seçimlik hareketlerle ilgili fiiller, tehlike suçu olarak görülmektedir." Bkz. A.e.
1286 Koca ve Üzülmez, a.g.e., s. 853
1287 Ancak Parlar-Hatipoğlu' nun da belirmiş olduğu gibi: "Sahte bir banka veya kredi kartından maksat, sahte olarak üretilen veya üzerinde sahtecilik yapılan banka veya kredi kartıdır. Diğer bir anlatımla suça konu olan kart tamamen sahte olabileceği gibi, üzerindeki bilgiler açısından da tahrifat yapılmış bir kart olabilir." Bkz. Parlar ve Hatipoğlu, a.g.e., s. 3769.
Soyaslan da: "Sahte banka veya kredi kartının üretilme şekli önemli değildir. Yeterki başkalarının hesabı üzerinde işlem yapmaya elverişli olsun. Sahte kart, üretimi itibariyle tümden sahte olabileceği gibi, önceden üretilmiş bir kart üzerinde yapılan değişiklikler de olabilir." Bkz. Soyaslan, a.g.e., s. 664.

edilmektedir.[1288] Doktrinde, sahte kartı sahteliğini "bilerek bulundurmak" hareketinin de cezalandırılır bir eylem olarak kabul edilmesi gerektiğini ve böylece tesadüflerin de cezalandırılmasının önlenebileceğinin belirtilmesinin[1289] yanında "bulundurmak" seçimlik hareketler arasında bulunmasa da "kabul etmek" fiilinin bulundurmayı da kapsadığını belirten yazarlar da bulunmaktadır.[1290]

Bu suçun oluşabilmesi için suça konu olan sahte banka veya kredi kartının başkalarına ait banka hesabıyla irtibatlandırılması gerekir.[1291] Zira, başkalarına ait bir hesapla ilişkili olmayan bir kartın hukuki sonuç doğurması mümkün olmamakla birlikte bu durumda fıkra kapsamında sahte bir karttan bahsedilemeyeceği için suçun oluşması da söz konusu olmayacaktır.[1292] Doktrinde başkalarına ait bir hesapla ilişkili olmayan bir kartın kullanılması suretiyle menfaat sağlanması halinde doktrinde dolandırıcılık suçu kapsamında değerlendirmenin yapılması gerektiği belirtilmekte[1293] olup kanaatimizce de bu şekilde bir yaklaşım gerçekleştirilebilecektir.

Ayrıca Yargıtay' ın da kabul etmiş olduğu üzere, suça konu olan sahte kart fiziksel varlığı olan kartları kapsadığı gibi internette kullanılmak üzere oluşturulan ve fiziksel varlığı olmayan sanal kartları da kapsamaktadır.[1294]

Doktrinde kredi veya banka kartına ilişkin sözleşmede veya sözleşme için ibraz edilen belgelerde sahtecilik yapılması halinde 5464 sayılı Kanun' un 37. m.' sinde suç olarak düzenlendiğinden suçun bu kapsamda değerlendirilmesi gerektiğini böyle bir durumda 245/2 nin gerçekleşmeyeceğini belirten yazarlar[1295] bulunmakla birlikte

1288 Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1046, 1047; Koca ve Üzülmez, a.g.e., s. 864.

1289 Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1047, 1048; Özbek, v.d., a.g.e., s. 973.

1290 Koca ve Üzülmez, a.g.e., s. 864; Mahmutoğlu, a.g.e., s. 874.

1291 Yaşar, Gökcan ve Artuç, a.g.e., s. 7348.

"…Esasen kartın işlevsel olabilmesi de buna bağlıdır. Yoksa olmayan bir hesaba ait kartın bir hukuki sonuç doğurması mümkün değildir. Bu durum belgede sahtecilik fiillerindeki "kandırıcılık kabiliyeti" kavramına benzemektedir. Diğer bir deyişle kanımızca kart başkasına ait gerçek bir banka hesabı ile ilişkilendirilmiş değil ise suçun oluşması da mümkün değildir. Zira bu halde madde anlamında sahte bir karttan söz etmek mümkün değildir." Bkz. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1048.

1292 Özbek, v.d., a.g.e., s. 973.

1293 Koca ve Üzülmez, a.g.e., s. 865.

1294 Akbulut, *Bilişim Alanında Suçlar*, s. 319;
Bkz. 'Yargıtay 11. Ceza Dairesi, 14.10.2010 t., E: 2008/20436, K: 2010/11188' (*Aktaran* Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 386, 387).

1295 "Nihayet sahteciliğin kredi ya da banka kartında yapılmış olması gerekir. Bunun dışındaki karta ilişkin sözleşmede sahtecilik yapılması madde kapsamına dahil değildir. Bu halde 5464 s. Kanun m.37/2'de yer alan suç düşünülmelidir." Bkz. Özbek, v.d., a.g.e., s. 974;
"Yine sahteciliğin konusunu banka veya kredi kartı değil de bu kartların verilmesi için yapılan sözleşme veya sözleşme için ibraz edilen belgelerin oluşturması halinde bu suç gerçekleşmez. Bu

böyle bir durumun varlığı halinde düzenlenen kartın gerçek bir kart olduğu bu kartın kullanılması suretiyle yarar sağlanmasının nitelikli dolandırıcılık suçunu oluşturduğunu belirten yazarlar[1296] da bulunmaktadır. Yargıtay' ın ise 5464 sayılı Kanun' un 37. m.' sinin ikinci fıkrasının dikkate alınmasını vurguladığı, ancak "5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 37/2. m.' sinde yer alan "kredi kartı, üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar, sözleşme imzalamak amacıyla sahte belge ibraz edenler" şeklindeki düzenlemenin sözleşmenin imzalanmasını da kapsayacak aşamaya kadar uygulanabileceği, kredi kartı sözleşmesinin düzenlenmesinden sonra kartın üretilmesi halinde 5237 sayılı TCK'nun 245/2. m.' sindeki suçu oluşturacağı" yönünde vermiş olduğu kararları bulunmaktadır.[1297] Bunun yanında Yargıtay gerçeğe aykırı beyan ve belgelerle ilgili banka veya kredi kurumundan kart çıkarılması fiilinin 245. m.' nin 2. fıkrası kapsamında olduğuna ilişkin kararları mevcuttur.[1298] Kanaatimizce gerçeğe aykırı

durumda 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 37. maddesinin 2. fıkrasında tanımlanan suçun oluştuğu söylenebilir." Bkz. Koca ve Üzülmez, a.g.e., s. 863.

1296 Soyaslan' a göre, "Yasa maddesinde "sahte oluşturulan veya üzerinde sahtecilik yapılan kartı kullanmak" ifadesi yer almaktadır. Oysa bu durumda sahte oluşturulan veya üzerinde sahtecilik yapılan bir kart bulunmamakta, fail tarafından banka ya da finans kurumuna verilen gerçek dışı bilgilerle "gerçek bir banka veya kredi kartının" oluşumu sağlanmakta ve bu kart gerçek kullanılmak suretiyle hukuka aykırı yarar sağlanmaktadır. Buna göre failin gerçeğe aykırı beyan ve sahte belgelerle elde ettiği banka kartı veya kredi kartını kullanması durumunda, TCK'nın 158. maddesinde düzenlenen nitelikli dolandırıcılık suçu oluşmaktadır." Bkz. Soyaslan, a.g.e., s. 664.

1297 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 387, 388.

"…Sanığın şikayetçiler K. ve T.'ın bilgilerini içeren suça konu asılları ele geçmeyen sahte kimliklerle T. adına katılan … Bank ve K. adına şikayetçi T…. Bank'a kredi kartı başvurusunda bulunup taleplerinin reddolunduğu kabul edilerek kurulan hükümde, sanığın K. kimliğiyle kredi kartı almak için başvurduğu şikayetçi T… Bank'ın cevabi yazısında, K. adına başvuru bulunmadığının bildirilmesi karşısında, bu husus ile birlikte anılan bankalardan başvuruların hangi gerekçeyle ve hangi aşamada reddedildiği sorulup 01.03.2006 tarihinde yürürlüğe giren 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 37/2. maddesindeki kredi kartı ile üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar ile sözleşme imzalamak amacıyla sahte belge ibraz edenler ile ilgili düzenlemenin sözleşme düzenlenmesine kadar olan safhada uygulanabileceği, kredi kartı sözleşmesinin düzenlenmesinden sonra kartın üretilmesi halinde eylemin 5237 Sayılı TCK'nun 245/2, kart banka tarafından üretilmeden sahteciliğin anlaşılması halinde bu suça teşebbüs, sahte üretilen bu kart kullanılarak menfaat temin edilmesi halinde ise aynı Kanunun 245/3. maddesinde yazılı suçun oluşacağı gözetilerek, eylemin 5464 Sayılı Kanunun 37/2. maddesi veya 5237 Sayılı TCK nun 245/2. madde-fıkrasında öngörülen suçları oluşturup oluşturmayacağının karar yerinde tartışılıp sonucuna göre hukuki durumlarının takdir ve tayini gerekirken eksik soruşturma ve uygun olmayan değerlendirme sonucu uygulama yeri olmayan 5237 Sayılı TCK nun 245/3. maddesiyle mahkumiyetine karar verilmesi,… BOZULMASINA" bkz. Yargıtay 11. Ceza Dairesi, 13.2.2013 tarihli, E: 2010/15673, K: 2013/2350, https://legalbank.net/arama, ET. 15 Temmuz 2020. Aynı yönde bkz. Yargıtay 11. Ceza Dairesi, 16.10.2007 tarihli, E: 2007/5158, K: 2007/6701; Yargıtay 11. Ceza Dairesi, 19.7.2010 tarihli, E: 2010/639, K: 2010/9199.

1298 "Sanığın, …ait nüfus cüzdanına kendi resmini yapıştırıp, bu nüfus cüzdanı ile bankaya müracaat ederek kredili mevduat hesabı başvuru formu imzalayıp bankaya sahte banka kartı ürettirmesi eyleminin kül halinde TCK.nun 245/2, 43 maddelerine uyduğu gözetilmeden yazılı şekilde TCK.nun 204/1. maddesi uyarınca eksik cezaya hükmedilmesi,…(BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 2.3.2015 tarihli, E: 2014/27246, K: 2015/12807, https://legalbank.net/arama, ET. 15 Temmuz 2020. Aynı yönde bkz. Yargıtay 8. Ceza Dairesi,

bilgi veya belgelerle banka veya kredi kartı çıkarılması halinde Dülger[1299] ve Akbulut[1300]' un da belirtmiş olduğu gibi banka görevlisinin araç olarak kullanılması başka bir deyişle dolaylı failliğin gerçekleşmesi suretiyle sahte kartın üretilmesi söz konusu olduğundan bu durumda 245. m.' nin 2. fıkrasının oluşacağını kabul etmek gerekir. Ancak Yargıtay' ın da belirtmiş olduğu gibi 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 37/2. m.' sinde yer alan düzenlemenin de sözleşmenin imzalanmasını kapsayacak aşamaya kadar uygulanabileceği göz önünde bulundurularak fikri içtima kurallarının uygulanarak çözüme gidilebileceği değerlendirilmektedir.

3.2.1.3.3.3. Sahte Oluşturulan veya Üzerinde Sahtecilik Yapılan Bir Banka veya Kredi Kartını Kullanmak Suretiyle Yarar Sağlanması (245/3)

245. m.' nin 3. fıkrasında yer alan suçun hareket unsurunu, failin "sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak" oluşturmaktadır.[1301] Bu fıkrada yer alan suçun oluşabilmesi için öncelikle banka veya kredi kartının sahte olarak oluşturulmuş veya üzerinde sahtecilik yapılmış bir kart bulunması gerekmektedir. Doktrinde sahte olarak oluşturulmamakla birlikte gerçeğe aykırı beyan veya belgelerle kart çıkarılması ve bu kartın kullanılarak yarar sağlanmasının da 245. m.' nin 3. fıkrası kapsamında değerlendirilmesi gerektiğini belirten yazarlar[1302] bulunmakla birlikte fail tarafından banka veya finans kurumuna verilen gerçeğe aykırı beyan veya belgelerle

30.3.2015 tarihli, E: 2014/28809, K: 2015/15294; Yargıtay 8. Ceza Dairesi, 24.3.2014 tarihli, E:2014/2222, K:2014/7240; Yargıtay 8. Ceza Dairesi, 14.1.2014 tarihli, E: 2013/455, K: 2014/579.

1299 "Sahte kart üretme hareketinin bizzat fail tarafından gerçekleştirilmesi gerekmez. Bankaya sahte belgelerle yapılan başvuru neticesinde banka görevlilerinin aldatılarak başkasının hesabıyla ilişkilendirilmek suretiyle sahte kartı üretilmesinin sağlanması halinde, banka görevlileri dolaylı fail, sahte belgeleri sunarak sahte kartın üretilmesini ve kendisine teslimini sağlayan kişi ise doğrudan fail olur ve bu durumda yalnızca doğrudan fail sorumludur." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 367.

1300 "…Burada sorun sahte belgelerle başvurarak kartın çıkarılmasında, dolaylı failliğin gerçekleşip gerçekleşmediğidir. Eğer dolaylı faillik kabul edilirse o zaman sahte belgelerle başvurup kartın çıkarılması durumunda sahte kart üretme fiili gerçekleşmiştir. Dolaylı failliğin gerçekleşeceğini düşünüyoruz. Zira banka görevlisinin araç olarak kullanılması suretiyle sahte belge üretilmektedir…" bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 322.

1301 Yaşar, Gökcan ve Artuç, a.g.e., s. 7350.

1302 Özbek, v.d., a.g.e., s. 979. "…Öte yandan bu halde 5464 s. Kanun m.37/2 hükmü de göz önünde bulundurulmalıdır." Bkz. A.e.

Karagülmez' e göre de: "… "sahte olarak oluşturulan" ifadesinden, kartın alınması sırasında sahte olarak verilen kullanıcı bilgilerine, gerçeğe aykırı kişisel bilgilere dayalı olarak düzenlenen kartlar anlaşılmalıdır." Bkz. Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 333.

"Maddenin üçüncü fıkrasında, "sahte olarak oluşturulan" ifadesinden kartın alınması sırasında sahte olarak verilen kullanıcı bilgileri, gerçeğe aykırı kişisel bilgilere dayalı olarak düzenlenen kartlar anlaşılmalıdır. Kart sahte olarak oluşturulmaktadır…" Bkz. Kurt, a.g.e., s. 187.

"gerçek bir banka veya kredi kartının" oluşumunun sağlandığını bu kartın kullanılarak yarar sağlanmasında 245/3 de yer alan suçun oluştuğunun kabul edilemeyeceğini belirten yazarlar[1303] da bulunmaktadır. Fıkrada açıkça belirtildiği üzere banka veya kredi kartı tamamen sahte bir kart şeklinde oluşturulabileceği gibi var olan kartın içerik olarak değiştirilmesi yolu ile de gerçekleştirilebilecektir.[1304] Başka bir anlatımla, bu fıkra kapsamında sahte kart, tamamen sahte olarak üretilen kartlar gibi fiziki olarak gerçek bir kart üzerine sahte bilgilerin girilmesi suretiyle de meydana getirilebilecektir.[1305] Bu doğrultuda, bir önceki başlık altında da açıklamış olduğumuz üzere gerçeğe aykırı belgelerle sahte kart oluşturulması 245. m.' nin 2. fıkrası kapsamında kabul edilebilecek olup bu kartın kullanılması ve haksız bir yarar elde edilmesi halinde 245. m.' nin 3. fıkrasında yer alan suçun da oluşacağının kabulü gerekir. Özbek vd.' nin de belirtmiş olduğu gibi bu durumda 5464 sayılı Kanun' un 37. m.' sinin 2. fıkrası hükmü de ayrıca göz önünde bulundurulmalıdır. Yargıtay Ceza Genel Kurulu kararından[1306] sonra Yargıtay' ın vermiş olduğu kararlar da bu yöndedir.[1307] Sahte olarak oluşturulan veya üzerinde sahtecilik yapılan söz konusu

1303 Bkz. Soyaslan, a.g.e., s. 664.
Parlar ve Hatipoğlu' na göre: "Sahte kart oluşturmak, gerçek kart üzerinde yapılanlar dışındaki sahtecilik fiillerini ifade etmektedir." Bkz. Parlar ve Hatipoğlu, a.g.e., s. 3769.
1304 Akbulut, *Bilişim Alanında Suçlar*, s. 333.
1305 Koca ve Üzülmez, a.g.e., s. 868, 869.
1306 "… 5237 sayılı TCY'nın 5377 ve 5560 sayılı Yasalar ile değişik 245. maddesinde düzenlenen "Banka ve kredi kartlarının kötüye kullanılması" suçu ise 765 sayılı TCY'nda bulunmayan bir suç türüdür. Maddenin getiriliş amacı gerekçede, "banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak" olarak açıklanmıştır… Sanığın ele geçirdiği başkasına ait nüfus cüzdanını kullanarak banka görevlilerince basımını sağladığı kredi kartı "sahte oluşturulan" kart niteliğinde olup bu kartın kullanılması suretiyle kendisine haksız yarar sağlaması eylemi daha ağır cezayı gerektiren başka bir suçu oluşturmadığından 5237 sayılı Yasanın 245/3.maddesinde düzenlenen suçu oluşturmaktadır. Burada sanığın eyleminin TCY'nın 158/1-j maddesinde düzenlenen dolandırıcılık suçunu oluşturabileceği düşünülebilir ise de, yasakoyucunun banka ve kredi kartları için getirdiği ve miktar olarak daha ağır cezayı gerektiren özel düzenleme nedeniyle bu maddenin olayda uygulanma yeri bulunmamaktadır. Bunun sonucu olarak ta 5237 sayılı TCY'nın olaya bir bütün olarak uygulanması halinde ortaya çıkacak sonuç ceza miktarı gözetildiğinde sanık hakkında 765 sayılı TCY hükümleri daha lehedir…" bkz. Yargıtay Ceza Genel Kurulu, 27.5.2008 tarihli, E: 2008/11-87, K: 2008/150, https://legalbank.net/arama, ET. 15 Temmuz 2020.
Yargıtay, 765 sayılı TCK döneminde ise bu tür olaylara 504/3. maddede yer alan nitelikli dolandırıcılık suçundan hüküm kurmaktaydı. "Sanığın babası, annesi ve kardeşi aına ilgili Banka Şubesi ile yaptığı kredi sözleşmelerine, onların haberi olmaksızın sahte imza atmak ve bu konuda hazırladığı sahte diğer belgeleri de sunmak suretiyle aldığı kredi kartlarıyla haksız kredi çektiğinin anlaşılması karşısında, eylemin TCK.nun 79. maddesinin yollamasıyla 504/1, 80. maddelerine uyan suçu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması,… BOZULMASINA" bkz. Yargıtay 6. Ceza Dairesi, 28.1.2002 tarihli, E: 2001/16683, K: 2002/693, https://legalbank.net/arama, ET. 15 Temmuz 2020.
1307 "Sanığın, Bekir Doğan'ın kimlik bilgilerine göre düzenlenmiş, üzerine kendi fotoğrafını yapıştırdığı sahte nüfus cüzdan talep belgesiyle sahte nüfus cüzdanı çıkartarak, sahte ikametgah belgesi de temin edip, mağdur bankaya başvurup sahte kredi kartı çıkartmak şeklindeki eyleminin

kartların bu fıkra kapsamında ayrıca bir belirleme yapılmadığından başka bir banka hesabı ile ilişkilendirilip ilişkilendirilmemesi arasında ise bir fark bulunmamaktadır.[1308]

Sahte olarak oluşturulan veya üzerinde sahtecilik yapılan kartın kullanılması suretiyle failin kendisine veya başkasına yarar sağlaması sağlaması gerekmekte[1309] olup yararın sağlanması ile suç tamamlanacaktır.[1310] Suçun tamamlanması için bir yarar elde edilmesi arandığından ve failin elde edeceği yarar mağdurun malvarlığında da bir zarar meydana getireceğinden bu suç netice bakımından bir zarar suçu niteliği taşımaktadır.[1311] Yararın ekonomik nitelikte olması gerekmekte olup bu yararın "fiilen elde edilmiş olması" şartı aranmamakta, üzerinde tasarruf edilebilecek durumda bulunması yeterli sayılmaktadır.[1312]

TCK.nun 245/2 ve 43. maddelerine uyan suçu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi,… (BOZULMASINA)" bkz. Yargıtay 8. Ceza Dairesi, 5.3.2014 tarihli, E: 2014/1217, K: 2014/5252, https://legalbank.net/arama, ET. 15 Temmuz 2020.

"Yargıtay kararında da belirtildiği üzere 245. maddenin 2. ve 3. fıkrası birbirinin nitelikli hali ya da unsuru olmayıp bağımsız suç tipleridir. Dolayısıyla 3. fıkra kapsamında yer alan sahte kart oluşturma hareketi 2. fıkrada olduğu gibi bir başkasının hesabı ile ilişkili olmak zorunda değildir…Ancak bu kartlar kullanılmamış ve dolayısıyla herhangi bir yarar temin edilmemişse kartı üretme fiilini icra hareketi olarak değerlendirip suça teşebbüsten bahsedebiliriz." Bkz. Mahmutoğlu, a.g.e., s. 875.

Yine Yargıtay vermiş olduğu bir başka kararda, sahte banka kartının, bu niteliğinin bilinerek üretilmiş veya kabul edilmiş hem de kullanılmış olunması durumunu, 245. maddenin 2. ve 3. fıkrası uyarınca cezalandırılmasına karar vermiştir. 'Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek ile sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak suçlarının birbirinden bağımsız iki ayrı suçu oluşturduğu gözetilmeyerek fikri içtima kurallarının uygulanması gerektiğinden bahisle tek suç kabulü ile eksik ceza tayini aleyhe temyiz olmadığından bozma nedeni yapılmamıştır.' 'Yargıtay 11. Ceza Dairesi, 29.5.2007 tarihli, E: 2007/2538, K: 2007/3738' (*Aktaran* Yaşar, Gökcan ve Artuç, a.g.e., s. 7350).

1308 Akbulut, *Bilişim Alanında Suçlar*, s. 333, 334; Yaşar, Gökcan ve Artuç, a.g.e., s. 7350.

"…bu kartın üretilmesinde başkasına ait yani gerçek bir hesapla ilişkili bilgiler kullanılacağı gibi, tamamen hayali kişiler adına açılmış bir hesapla ilgili bilgiler de söz konusu olabilir." Bkz. Koca ve Üzülmez, a.g.e., s. 869.

1309 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6977; Akbulut, *Bilişim Alanında Suçlar*, s. 337.

1310 Yaşar, Gökcan ve Artuç, a.g.e., s. 7351.

1311 "…Ancak tipte sadece bir yarar elde edilmesinden söz edildiğine göre suçun oluştuğunu kabul bakımından bir zararın da oluşup oluşmadığını incelemeye gerek bulunmadığı düşüncesindeyiz." Bkz. Özbek, v.d., a.g.e., s. 978.

1312 Yaşar, Gökcan ve Artuç, a.g.e., s. 7351; Özbek, v.d., a.g.e., s. 978; Akbulut, *Bilişim Alanında Suçlar*, s. 337.

"...bu yararın gelir artırıcı olması yanında bir borçtan kurtulmak yönünde olması da mümkündür." Bkz. Özbek, v.d., a.g.e., s. 978.

"…bir kişinin kendi adına hesap açıp, daha sonra bu hesaba başka hesaplardan sahte banka veya kredi kartını kullanmak suretiyle para transferi yapması durumunda suç tamamlanmıştır. Gidip bankadan bu paraları alması gerekmez." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 337.

Son olarak belirtmek gerekir ki, bu suçun oluşabilmesi için failin fıkrada belirtmiş olan fiilinin TCK' da veya başka bir Kanun' da daha ağır cezayı gerektiren bir suç oluşturmaması gerekmektedir.[1313]

3.2.3.3. Manevi Unsur

245. m.' lerde düzenlenmiş olan suçların her biri açısından manevi unsuru kast oluşturmakta olup fiillerin taksirli hali suç olarak düzenlenmediğinden taksirli halden cezalandırma söz konusu olmayacaktır.[1314] Maddede yer alan suçlar doğrudan kastla işlenebileceği gibi olası kastla da işlenebilecek[1315] olup suç tipinde fiilin belli bir saikle işlenmesi hali aranmadığından bu suçta özel kast aranmayacaktır.[1316]

3.2.3.4. Hukuka Aykırılık

245. m.' nin birinci fıkrası kapsamında, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası fiili suç olmaktan çıkarmaktadır. İlgili başlıkta da belirtmiş olduğumuz gibi burada rızanın varlığı tipikliğin bir unsuru olarak suçun unsurlarından kabul edilmelidir.[1317] Ancak doktrinde rızanın varlığını hukuka uygunluk sebebi sayan yazarlar da bulunmaktadır.[1318] Bunun yanında, hukuka uygunluk sebepleri içinde yer alan meşru savunma, hakkın kullanılması ve kanun hükmünün yerine getirilmesi hukuka uygunluk sebeplerinin bu suç bakımından uygulanması söz konusu olmayıp suç tipinde düzenlenmiş olan fiilleri hukuka uygun hale getirmeyecektir.[1319]

3.2.3.5. Unsurların Dışında Kalan ve Cezalandırılmaya Etkili Olan Şartlar

3.2.3.5.1. 245. Maddenin 1. Fıkrasında Yer Alan Suç Açısından Şahsi Cezasızlık Sebebi

TCK' nın 245. m.' sinin 4. fıkrası:

"Birinci fıkrada yer alan suçun;

1313 Parlar, Hatipoğlu, a.g.e., s. 3769; Yaşar, Gökcan ve Artuç, a.g.e., s. 7351.
1314 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6978; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 400; Parlar ve Hatipoğlu, a.g.e., s. 3770.
1315 Yaşar, Gökcan ve Artuç, a.g.e., s. 7352.
1316 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6978; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 400; Parlar ve Hatipoğlu, a.g.e., s. 3770.
1317 Aynı yönde bkz. Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1034.
1318 Ayrıntılı bilgi için bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 400-402; Parlar ve Hatipoğlu, a.g.e., s. 3770.
1319 Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1034; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 402.

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz."[1320]

şeklinde düzenlenmiştir.

Böylece mala karşı işlenen suçlarda olduğu gibi (TCK m. 167/1) bu suç bakımından da bazı akrabalık ilişkileri "şahsi cezasızlık sebebi"[1321] olarak kabul edilmiş[1322] olup böyle bir düzenlemeye hükümde yer verilmesi bu suçun esasen malvarlığına karşı işlenen bir suç ve korunan hukuki yararın kişinin malvarlığı üzerindeki hak veya hakları olduğunun üstü kapalı bir kabulü olduğunu göstermektedir.[1323]

5377 sayılı Kanun ile gerçekleştirilen değişiklikle 245. m.' ye eklenen 4. fıkra düzenlenmesi sadece 245. m.' nin 1. fıkrasında yer alan suç için geçerli[1324] olup suçun fıkrada belirtilen akrabalarla birlikte başka şahıslarla iştirak halinde işlenmesi durumunda, şahsi cezasızlık sebebi sadece akraba olan fail hakkında uygulanacaktır.[1325] Şahsi cezasızlık sebebinden yararlanan ilgili akraba hakkında ise CMK'nın 223/4-b bendi uyarınca ceza verilmesine yer olmadığına karar verilecektir.[1326]

3.2.3.5.2. 245. Maddenin 1. Fıkrasında Yer Alan Suç Açısından Etkin Pişmanlık

5560 sayılı Kanun ile TCK' nın 245. m.' sine "Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır" hükmü 5. fıkra olarak eklenmiş olup böylelikle malvarlığına karşı suçlarda etkin pişmanlığı düzenleyen TCK' nın 168. m.' sinin uygulanma imkanı

1320 https://mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf, ET. 30 Mart 2020.

1321 "Bilindiği gibi şahsi cezasızlık nedeni fiilin haksızlık içeriğini etkilemeyen, kusurla ilgili olmayan bir husustur. Kanun koyucu bazı suçlarda belirli akrabalar arasında işlenen fiillerin yarattığı zararın aile içinde giderilebileceğini veya bu tür fiillerin aile içinde mazur görülebileceğini kabul ederek, aile içi barışı koruma düşüncesiyle şahsi cezasızlık nedenine yer verebilmektedir. Bu belirlemeler suçun kişilerin zararına işlendiği fiiller için geçerlidir. Bir başka ifadeyle belirli kişi veya kişilerin zararına işlenen suçlarda, bu suçlar belirli akrabalık ilişkisi içinde bulunan kişilere karşı işlendiğinde şahsi cezasızlık nedeni kabul edebilmektedir…" bkz. Akbulut, *Bilişim Alanında Suçlar,* s. 304.

1322 Koca ve Üzülmez, a.g.e., s. 855; Akbulut, *Bilişim Alanında Suçlar,* s. 304.

1323 Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", s. 1036.

1324 Yaşar, Gökcan ve Artuç, a.g.e., s. 7352.

1325 Koca ve Üzülmez, a.g.e., s. 855; Akbulut, *Bilişim Alanında Suçlar*, s. 305; Yaşar, Gökcan ve Artuç, a.g.e., s. 7353.

1326 Parlar ve Hatipoğlu, a.g.e., s. 3770.

getirilmesiyle söz konusu suç malvarlığına karşı işlenen suçlara daha fazla yakınlaştırılmıştır.[1327]

TCK'nın 168. m.' si[1328] hükmü çerçevesinde, failin etkin pişmanlık hükmünden yararlanabilmesi için, suçun tamamlanmış olması, failin, suça azmettirenin ya da yardım edenin bizzat pişmanlık göstermesi suretiyle mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle gidermesi, kısmen giderme söz konusu olduğunda ise mağdurun buna rıza göstermesi, kovuşturmadan önce veya kovuşturma başlamışsa hüküm verilmeden önce aynen iade veya tazminin sağlanması gerekmektedir.[1329] O zaman, 245. m.' nin birinci fıkrasındaki suç tamamlandıktan sonra ancak hakkında kovuşturma başlamadan önce failin, azmettirenin veya yardım edenin bizzat pişmanlık göstermesi suretiyle mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde verilecek cezanın üçte ikisine kadarı indirilecek, etkin pişmanlığın kovuşturma başladıktan sonra ancak hüküm verilmeden önce gösterilmesi halinde ise verilecek ceza yarısına kadar indirilecektir.[1330]

3.2.3.6. Kusurluluk

Söz konusu suç tipi kusurluluk açısından ayrı bir özellik arz etmemektedir.

1327 Yaşar, Gökcan ve Artuç, a.g.e., s. 7355.

1328 "Etkin pişmanlık
Madde 168 –
(1) Hırsızlık, mala zarar verme, güveni kötüye kullanma, dolandırıcılık, hileli iflâs, taksirli iflâs suçları tamamlandıktan sonra ve fakat bu nedenle hakkında kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde, verilecek cezanın üçte ikisine kadarı indirilir.
(2) Etkin pişmanlığın kovuşturma başladıktan sonra ve fakat hüküm verilmezden önce gösterilmesi halinde, verilecek cezanın yarısına kadarı indirilir.
(3) Yağma suçundan dolayı etkin pişmanlık gösteren kişiye verilecek cezanın, birinci fıkraya giren hallerde yarısına, ikinci fıkraya giren hallerde üçte birine kadarı indirilir.
(4) Kısmen geri verme veya tazmin halinde etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranır.
(5) Karşılıksız yararlanma suçunda, fail, azmettiren veya yardım edenin pişmanlık göstererek mağdurun, kamunun veya özel hukuk tüzel kişisinin uğradığı zararı, soruşturma tamamlanmadan önce tamamen tazmin etmesi halinde kamu davası açılmaz; zararın hüküm verilinceye kadar tamamen tazmin edilmesi halinde ise, verilecek ceza üçte birine kadar indirilir. Ancak kişi, bu fıkra hükmünden iki defadan fazla yararlanamaz." Bkz. https://mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf, ET. 30 Mart 2020.

1329 Artuk, Gökcen ve Yenidünya, *Türk Ceza Kanunu Şerhi: Madde 234-345*, s. 6981.

1330 Koca ve Üzülmez, a.g.e., s. 855, 856.

3.2.4. Yasak Cihaz ve Programların Üretilmesi ve Ticareti Suçu (TCK madde 245/A)

24.3.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu' nun 30. m.' sinin 5. fıkrasıyla TCK' nın "Bilişim Alanında Suçlar" bölümüne eklenen "Yasak cihaz veya programlar" başlıklı 245/A m.' si şu şekilde düzenlenmiştir:

> *"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".*[1331]

Söz konusu madde, AKSS' nin "Cihazların Kötüye Kullanımı" başlıklı 6. m.' sinin getirmiş olduğu yükümlülüğün[1332] karşılanması amacıyla ceza mevzuatımıza eklenmiştir.[1333] Nitekim, bilişim suçlarıyla mücadele etmek için sadece suçların yaptırıma bağlanmasının yetmeyeceği, bu suçların işlenmesini sağlayan ve kolaylaştıran programların, cihazların, kodların suç işlemek amacıyla imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, satışa arz edilmesi gibi kaynağında fiillerin yasaklanması gerektiği görüşünün egemen olduğu belirtilmektedir.[1334] 245/A m.' sinde yer alan fiillerin tanımlanmasıyla da bilişim sistemlerinin ve bu sistemlerde yer alan verilerin daha etkin şekilde korunması amaçlanarak dar veya geniş anlamda bilişim suçlarının işlenmesi bakımından esasen hazırlık hareketi mahiyetindeki cihaz veya şifre üretimi ve ticareti fiilleri bağımsız suç olarak düzenlenmiştir.[1335] Sözleşme, 6. m.' nin uygulanacağı suçları, yasadışı erişim, yasadışı araya girme, verilere

1331 https://mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf, ET. 30 Mart 2020.

1332 "Bu yükümlülük, örneğin Windows işletim sisteminde genellikle "sömürü" (expolits) olarak adlandırılan ve bir başka kişinin sistemine kötücül yazılımları tanıtmak için kullanılan yazılım gibi bir uygulama yazılımının bilinen bir zayıflığı ya da kırılganlığı hakkında bilgiler gibi araçları suç olarak tanımlamayı içermektedir. Söz konusu madde, bilişim suçlarının kaçınılmaz bir özelliği haline gelen ve "kötücül pazar yeri" olarak tanımlanan "bilişim korsanları için araç" pazarlanmasını suç haline getirmek için tasarlanmıştır." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 453.

"…Bilişim suçları herhangi bir cihaz veya programdan veya koddan yararlanmaksızın da işlenebilmekle birlikte çoğunlukla bu tür cihaz veya program veya verilerle işlenmektedir. Hatta suç işlemede kullanılan bu araçların elde edilmesine yönelik olarak, üretim ve dağıtımları alanında "deepweb"te oluşan bir karaborsanın bulunduğu belirtilmektedir. Nitekim bu fiilin Sanal Ortamda İşlenen Suçlar Sözleşmesinde düzenlenmesi nedenlerinden biri de, bilişim suçlarını işlemek için bu tür araçların elde edilmesine yönelik, üretim ve dağıtımları alanında karaborsanın oluşmasına yol açabilecek güçlü bir eğilimin bulunmasıdır." Bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 347.

1333 Koca ve Üzülmez, a.g.e., s. 870, 871.

1334 Akbulut, *Bilişim Alanında Suçlar*, s. 347.

1335 Koca ve Üzülmez, a.g.e., s. 871.

müdahale ve sisteme müdahale olarak belirlemişken her ne kadar "245/A" olarak düzenlenmişse de Ceza Kanunumuzda yer alan bu düzenleme sadece 245. m.' ye ilişkin bir düzenleme olmayıp "Bilişim Alanında Suçlar" bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar için de uygulanması kabul edilmiştir.[1336]

AKSS' de, belirlenen fiillerin suç işlemek amacıyla gerçekleştirilmemesi halinde ceza sorumluluğunun gerçekleşmemesi gerektiği belirtilmiş olup bu ifadenin, akademik veya ticari açıdan hukuka uygun işlemleri gerçekleştirmek için veri güvenliği alanında çalışan ve söz konusu araçları kullanabilen kişileri korumak için zorunlu olduğu belirtilmektedir.[1337]

Öğretide, madde başlığının eylem unsurunu ön plana çıkarması gerekirken bu maddede suçun konusunun ön plana çıkarıldığı bu sebeple madde başlığının içeriğe uygun olmadığı belirtilerek "suçta kullanılacak cihaz veya programların üretilmesi, yayılması veya bulundurulması"[1338] veya 245. m.' deki gibi "program veya cihazların kötüye kullanılması"[1339] gibi fikirler ileri sürülmüş olup biz de madde başlığının içeriğe uygun olarak düzenlenmesi gerektiği fikrine katılıyoruz.[1340]

3.2.4.1. Korunan Hukuksal Değer

Suç tipinde, "Bilişim alanında suçlar" bölümünde düzenlenen suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların daha kolay işlenmesini sağlayabilen cihaz, program, şifre ve güvenlik kodlarının üretilmesi ve tedavüle sokulmasının yasaklanmış olduğu[1341] 245/A m.' sinin koruduğu hukuksal yarar, "bilişim sistemlerinin güvenliği ve güvenilirliği"[1342] (bu sistemlere karşı toplumda oluşan güven[1343]) yanında bilişim sistemleri aracılığıyla işlenebilecek diğer suçların koruduğu hukuksal değerlerdir.[1344]

1336 Akbulut, *Bilişim Alanında Suçlar*, s. 346; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 454.
1337 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 453.
1338 Özbek, v.d., a.g.e., s. 1066.
1339 Akbulut, *Bilişim Alanında Suçlar*, s. 348.
1340 Aynı yönde bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 454.
1341 Koca ve Üzülmez, a.g.e., s. 871.
1342 Aynı yönde bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 349.
1343 Aynı yönde bkz. Koca ve Üzülmez, a.g.e., s. 871.
1344 Aynı yönde bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 455, 456.

3.2.4.2. Maddi Unsur

3.2.4.2.1. Fail ve Mağdur

Suçun faili açısından herhangi bir özellik aranmadığından herkes bu suçun faili olabilecektir.[1345] Bunun yanında, suç tipinde yer alan cihazları satma veya başkalarına verme hareketleri, karşısında bunları satın alan veya kabul eden failleri gerektirdiğinden bu hareketler bakımından söz konusu suç çok failli suç özelliği taşır.[1346]

245/A m.' sinde yer alan suç hazırlık hareketi niteliğindeki fiilleri yaptırım altına aldığından ve henüz belirlenebilir faili bulunmadığından bu suç açısından mağdur, toplumu oluşturan herkestir.[1347] Zira, maddede düzenlenen fiillerin gerçekleştirilmesi ile belirli bir kişinin ya da kişilerin zarar görmesi söz konusu değildir.[1348]

3.2.4.2.2. Suçun Konusu

Suçun konusunu oluşturan "cihaz, bilgisayar programı, şifre veya sair güvenlik kodu", "Bilişim Alanında Suçlar" bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması aracılığıyla işlenen suçların işlenmesi amacıyla yapılmış olmasının yanında suçun işlenmesine de elverişli olmadırlar.[1349]

Cihaz, her türlü donanımı, bilgisayar programı yazılımı, şifre, dijital sembollerden oluşan ve sisteme ulaşımı sağlayan anahtarı, sair güvenlik kodu ise şifre dışında ses, retina, parmak izi vb. güvenlik unsurlarını ifade etmektedir.[1350]

3.2.4.2.3. Fiil

245/A m.' sinde yer alan suç, suçun konusunu oluşturan cihaz, program, şifre veya sair güvenlik kodunu imal etme, ithal etme, sevk etme, nakletme, depolama, kabul etme, satma satışa arz etme, satın alma, başkalarına verme veya bulundurma hareketlerinin herhangi birisinin yapılmasıyla gerçekleşebileceğinden seçimlik hareketli[1351], suç ile bir zararın oluşması gerekmediğinden soyut tehlike,

1345 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 456; Koca ve Üzülmez, a.g.e., s. 872; Akbulut, *Bilişim Alanında Suçlar*, s. 349.
1346 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 456; Koca ve Üzülmez, a.g.e., s. 872; Akbulut, *Bilişim Alanında Suçlar*, s. 350.
1347 A.e.
1348 Akbulut, *Bilişim Alanında Suçlar*, s. 350.
1349 Koca ve Üzülmez, a.g.e., s. 872; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 457.
1350 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 457.
1351 Koca ve Üzülmez, a.g.e., s. 873.

gerçekleştirilen hareketlerin sonucunda bir neticenin gerçekleşmesi aranmadığı için de sırf hareket suçudur.[1352] Madde metninde belirtildiği üzere, suçu oluşturan hareketler ise bilişim alanında suçlar bölümünde yer alan veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesinde kullanılması amacıyla gerçekleştirmiş olması gerekir.[1353] AKSS' nin 6. m.' sinde kişilere ceza sorumluluğunun yüklenebilmesi için belirli sayıda aracın gerekli olması yönünde taraf devletlere düzenleme yapmaları hususunda izin vermekte ise de 245/A m.' sinde yer alan mezkur hükümde sayısal bir sınırlandırmaya yer verilmemiştir.[1354]

3.2.4.3. Manevi Unsur

245/A m.' sinde yer alan suç ancak kasten işlenebilen bir suç olup taksirle işlenmesi mümkün değildir.[1355] Ancak suçun oluşabilmesi için kastın varlığı yeterli olmayıp failin suçu oluşturan hareketleri bilişim alanında suçlar bölümünde yer alan veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesinde kullanılması amacıyla gerçekleştirmiş olması gerekir.[1356] Bu suçta amaç unsuru arandığından olası kastla gerçekleştirelemeyecek olup suçun oluşması içinse amaç suçun gerçekleşmesi şartı aranmamaktadır.[1357]

3.2.4.4. Hukuka Aykırılık

245/A m.' sinde yer alan suç için kanunun verdiği yetki, görevin ifası ve hakkın kullanılması hukuka uygunluk sebepleri olarak kabul edilebilecek olup CMK' nın 134. m.' sinde yer alan bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri, özel adli bilişim laboratuarları ya da bilişim güvenliği şirketlerinde söz konusu suçun konusunu oluşturan cihaz veya programların bulundurulması buna örnek olarak verilebilecektir.[1358] İlgilinin rızası, kişilerin üzerinde mutlak surette tasarruf edebileceği haklar üzerinde bulunduğundan, meşru

1352 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 458.
1353 Koca ve Üzülmez, a.g.e., s. 873; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 458. "Bilişim sistemlerinin güvenliğinin test edilmesi için belirli aralıklarla "pentest" yapılır. Bu testlerin yapılması için cihaz ya da program üretilmesi ve bulundurulması halinde bu suç oluşmaz." Bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 459.
1354 A.e.; Akbulut, *Bilişim Alanında Suçlar*, s. 346.
1355 Koca ve Üzülmez, a.g.e., s. 873; Akbulut, *Bilişim Alanında Suçlar*, s. 358.
1356 Koca ve Üzülmez, a.g.e., s. 873; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 458.
1357 Koca ve Üzülmez, a.g.e., s. 873; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 458; Akbulut, *Bilişim Alanında Suçlar*, s. 358.
1358 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 459; Koca ve Üzülmez, a.g.e., s. 874; Akbulut, *Bilişim Alanında Suçlar,* s. 359.

savunma ile de bireysel hukuki değerler korunduğundan bu suç tipi bakımından meşru savunma ve ilgilinin rızası hukuka uygunluk sebeplerinin uygulanmayacağı kabul edilmelidir.[1359]

3.2.4.5. Kusurluluk

Söz konusu suç tipi kusurluluk açısından ayrı bir özellik arz etmemektedir.

1359 Akbulut, *Bilişim Alanında Suçlar*, s. 358, 359.

SONUÇ

Bilişim teknolojilerinin dinamik ve hızla gelişen yapısı sebebiyle bu alanda gerçekleşen ihlallerin de aynı hızla yeni ihlal türlerini beraberinde getirmesi bu alana ilişkin olarak gerçekleştirilecek olan düzenlemelerin de bir o kadar güncel tutulmasını gerektirebileceğinin, bu teknolojilerin bir getirisi olan bilişim sistemlerinin hayatın vazgeçilemez unsurları olarak kabulü karşısında belki de ceza kanunlarında yer alan diğer klasik suç türlerine nazaran toplumun geneline yansıyan daha yıkıcı sonuçlar doğuracak etkilerinin olabileceği kabul edilebilecektir.

Çalışmamızın sonuç kısmında, çalışma konumuzu oluşturan 5237 sayılı TCK' nın "Bilişim Alanında Suçlar" bölümünde yer alan suç tiplerinin incelenmesi, teknolojide gelinen güncel durumun da göz önüne alınarak değerlendirilmesi sonucunda bir takım önerilerde bulunulacaktır.

Öncelikle, 5237 sayılı TCK' nın 243. m.' sinde "bilişim sistemi" kavramının benimsenmiş olması, hızla gelişen ve yaşamımızın neredeyse her alanına nüfuz eden teknolojik gelişmeler karşısında kapsayıcı bir terim olması açısından doğru bir yaklaşımdır. Bununla birlikte 243. m.' nin gerekçesinde yer alan "verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma imkanı veren manyetik sistemler" tanımının "bilişim sistemi" kavramını açıklamada yeterli olmadığı görülmektedir. çok hızlı değişen, gelişen ve sınırları belli olmayan bilişim alanına ilişkin statik ve sınırları daraltıcı nitelikte tanımlama çalışmalarının doğru sonuçlar doğurmayacağı bir gerçek olmakla birlikte kanunilik ve belirlilik ilkelerinin geçerli olduğu ceza hukukunda bu suç tiplerine ilişkin kendilerine özgü yapıları dikkate alınmak suretiyle en azından muğlak olmayan kapsayıcı belirlemelerin yapılması gereği de göz ardı edilmemelidir. Bu anlamda, "bilişim sistemi" kavramının tanımının yapılmasından ziyade taşıması gereken unsurları belirleme yönteminin daha uygun olacağını, kanun maddesinde yer alan "bilişim sistemi" ifadesinin her somut olayda ve güncel gelişmeler dikkate alınmak suretiyle ve yukarıda ayrıntılı olarak belirtmiş olduğumuz unsurların varlığı veya yokluğu değerlendirilmek

suretiyle tekraren yorumlanması gerektiğini düşünmekteyiz. Ayrıca, gelişen teknoloji ile birlikte ortaya çıkan yeni sistemlerin varlığı, (akıllı telefonlar, tabletler, akıllı cihazlar vb.) bilişim suçlarının günümüzde sadece bilgisayarlarla değil bilişim temelli bu cihazlarla da işlenilebilmesi, 5237 sayılı TCK' nın 243. m.' sinin gerekçesinde yer alan bilişim sistemi kavramının tanımının güncellenmesini kaçınılmaz hale getirmektedir. Zira, günümüzde yeni dijital ve akıllı üretim teknolojileri ile ortaya çıkan "nesnelerin interneti" sağlıktan, endüstriye, ulaşım ve kamu hizmetlerinden, bina ve ev otomasyonuna kadar etki alanı yaratacak iken bir bilişim sisteminin, sadece verileri toplayıp yerleştirme sonrasında bunları otomatik işleme tabi tutabilme özelliklerini içereceğinin kabulü günümüz teknolojisine ve koşullarına uymamaktadır. Bu bağlamda, bir bilişim sisteminin söz konusu unsurların yanı sıra veriyi gönderebilme (iletebilme/aktarabilme) özelliğini de ihtiva ettiği gerçeğinin gerekçede yer alan tanıma eklenmesi doğru bir yaklaşım oluşturacaktır. Diğer taraftan, gerekçede yer alan tanımda "manyetik sistem" ifadesinin, bilişim sistemlerini ifade etmede yanlış bir ifade oluşturmadığı değerlendirilse de bir bilişim sistemini tanımlamada belirleyici bir unsur niteliği taşımadığı ve mevcut tanımdan çıkartılmasının da uygun olacağı düşünülmektedir.

Bilişim teknolojilerinde yaşanan gelişmelerin geldiği nokta ve ilerleme hızı göz önünde bulundurulduğunda, ulusal siber güvenliğin sağlanmasının ulusal güvenliğin bir parçası olarak görüldüğü ülkemizde bu bağlamda hem teknik olarak güvenliğin sağlanması hem de mevzuat açısından ciddi çalışmalar yapıldığı görülmektedir. Zira, güvenliğin geri planda bırakıldığı bir sistemin sonradan güvenli hale getirilmesinin daha zor olacağı ve istenilen ölçüde gerçekleştirilemeyeceği fikrinden hareketle öncelikle veya eş zamanlı olarak suç öncesi güvenliğin sağlayacak düzenlemelerin, bir suçun varlığı halinde ise bununla en etkili biçimde mücadeleyi gerektiren hukuki altyapının oluşturulması gerekmektedir. Siber güvenliğin ulusal güvenliğin bir parçası olduğunun kabulü karşısında ulusal ceza mevzuatımıza bakıldığında ise açık bir boşluk olduğu görülmektedir. Siber güvenlik, kritik altyapılar ve siber terörizm kavramlarının esasen birbirinden ayrılamaz kavramlar olduğu görülmektedir. Terör konusunda yıllardır ciddi yaralar almış bir ülke olarak değişen ve gelinen noktada siber terörizme dönüşen eylemlere karşı ceza hukuku anlamında da bir takım düzenlemeler yapılması gerektiği açıktır. Bu anlamda doktrinde yer alan bilişim sistemlerinden yararlanılması suretiyle terör eylemlerinin gerçekleştirilmesinin ilgili suç tipi açısından cezayı artıran nitelikli hal sayılması gerektiği fikrine katılmakla beraber

TCK' nın onuncu bölümünde yer alan "Bilişim alanında suçlar" bölümü altında düzenlenmiş olan suç tipleri arasında mevcut hükümler arasında en uygun madde olduğu düşünülen 244. m.' ye 244/A şeklinde bir m. eklenerek (veya ilgili bölümlerde de belirtildiği üzere 243 ile 244. m.' nin ortak bir m.' de birleştirilmesi sonucu oluşturulacak olan yeni maddeye göre) kritik altyapıları hedef alan siber terör eylemlerinin ayrı bir suç olarak düzenlenebileceğini düşünmekteyiz. Bunun yanında 12 Nisan 1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu' nun "Terör suçları" başlıklı 3. m.' sine 2. fıkra olarak TCK' ya eklenmesini önerdiğimiz 244/A m.' si siber terör suçu olarak eklenerek TCK ile arasındaki bağlantının sağlanabileceği ayrıca "Cezaların artırılması" başlıklı 5. m.' ye de bilişim sistemlerinden yararlanılması suretiyle terör eylemlerinin gerçekleştirilmesinin cezayı artıran nitelikli hal olarak eklenmesi böylelikle çoklu ve tam bir koruma sağlanmasının yanında siber terör eylemi niteliğinde kabul edilebilecek eylemlerin ayrıca yaptırım altına alınması sonucunda caydırıcılık noktasında ileri bir aşamada kaydedilebileceği değerlendirilmektedir.

Yukarıda yer alan açıklamalarımıza ek olarak siber savaş, siber terör, siber silahlar gibi tanımların üzerinde ise küresel bir uzlaşı zor olsa da siber uzayın barışçıl kullanımı için uluslararası işbirliği, küresel standartlar ve normların oluşturulması, bir uzlaşı tesisi edilmesi için devletlerarası siber alana özgü geliştirilmiş ortak ve teknik bir dilin kullanımı, siber uzay alanı üzerinde devletlerarasındaki mücadelenin artması ile siber güvenlik konusunda uluslararası ilişkiler disiplinin ve güvenlik çalışmalarının analizi bunun yanında gerek uluslararası ve ulusal gerek kurumsal güvenlik açısından farklı disiplinleri içine alacak multidisipliner siber mücadele kavramı geliştirilerek bilimsel ve akademik literatüre katkıda bulunulması gerektiği de vurgulanması gereken başka bir nokta olduğu düşünülmektedir.[1360]

765 sayılı TCK' nın 525/c m.' sinde "Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutma bir sisteme, verileri veya diğer unsurları yerleştirme veya var olan verileri, diğer unsurları tahrif etme" şeklinde suç olarak düzenlenen verilerde sahtecilik suçuna TCK' da yer verilmemiş bunun yanında AKSS' nin 7. m.' sinde düzenlenen bilgisayarla bağlantılı sahtecilik suçunun karşılığı da mevzuatımızda düzenlenmemiştir. Bu bağlamda, bilişim sisteminde yer alan verilere müdahale suretiyle sahte bir belge

1360 Çelik, a.g.e., s. 118.

oluşturulmasına esas olması halinin belgede sahtecilik suçları açısından cezayı artırıcı nitelikli hal olarak kabul edilebilecektir. Zira, çalışmamız boyunca benimsemiş olduğumuz görüşe göre, "bilişim alanında suçlar" bölümünde dar anlamda bilişim suçları düzenlenmiş olduğundan, bilişim sistemleri aracılığıyla veya verilere müdahale suretiyle gerçekleştirilecek olan ihlallerin ise ilgili suç tipinin koruduğu hukuksal değer göz önünde bulundurularak ilgili maddeye nitelikli hal olarak işlenmesi esasının benimsenmesi gerektiği kabul edilmektedir.

AKSS' nin 7. m.' sinde düzenlenen bilgisayarla bağlantılı sahtecilik suçunun karşılığının bulunmadığı görülmekte olup AKSS' nin ilgili maddesinin mevzuatımızda düzenlenmesinin de isabetli olacağını düşündüğümüzü belirtmek isteriz. Bu bağlamda, bilişim sisteminde yer alan verilere müdahale suretiyle sahte bir belge oluşturulmasına esas olması hali belgede sahtecilik suçları açısından cezayı artırıcı nitelikli hal olarak kabul edilebilecektir.

TCK' nın yedinci bölüm genel ahlaka aykırı suçlar başlığı altında 226. m.' sinde müstehcenlik suçu yer almakta ise de çocuk pornografisine ilişkin olarak özellikle AKSS' nin "Çocuk pornografisiyle bağlantılı suçlar" başlıklı ilgili maddesi örnek alınarak ayrı bir suç tipi olarak düzenlenmeyişinin Türk Ceza Hukuku açısından önemli bir eksiklik oluşturduğu bilişim teknolojilerinin geldiği nokta düşünüldüğünde, bilişim sistemlerinin hayatımızın her alanına dahil olan "bilişim sistemleri kullanımının" TCK' nın 226. m.' si içerisine eklenmesi ve böylelikle güne uygun şekilde güncellenmesi gerektiği değerlendirilmektedir.

TCK' nın 243. m.' sinin birinci fıkrasında yer alan bilişim sistemine girme suç tipinde yer alan "girmek" fiili yerine, madde düzenlemesi ile korunmak istenen değer ve maddenin düzenleniş amacı dikkate alındığında mukayeseli hukukta "yetkisiz erişim", "zorla erişim", "hileyle erişim" gibi farklı kavramlarla kullanıldığı da göz önünde bulundurulduğunda terminoloji açısından izinsiz veya yetkisiz erişim ifadesinin kullanılması daha uygun olacaktır. Kaldı ki, 243. m.' nin başlığında tercih edilen "bilişim sistemine girme" suçu Avrupa Siber Suç Sözleşmesi'nin 2. m.' sinde öngörülen hukuka aykırı erişim suç tipi düzenlemesi de dikkate alındığında gerçekleştirilecek olan değişiklikle mukayeseli hukukla uyumlu hale gelecektir. Bunun yanında sadece ve başlı başına bilişim sistemine girmenin suç olarak düzenlenmiş olduğu 243. m. etkili ve yerinde olsa da tasarılarda yer aldığı hali ile teşebbüs halinde kalan hareketlerin de tamamlanmış suçtan cezalandırılması esasının benimsenmesinin eylemleri önlemede daha etkin sonuçlar doğuracağı ve suçla

mücadelede daha etkili olacağını düşünmekteyiz. Nitekim, Alman Ceza Kanunu' nda yer alan düzenlemelere bakıldığında da düzenlenen birçok suç tipide teşebbüs halinde kalan suçun cezalandırılacağına vurgu yapıldığı görülmektedir.

TCK' nın 243. m.'sinde düzenlenmiş olan suçun maddi konusunu oluşturan bilişim sistemlerinin kamu veya özel hukuk tüzel kişisine ve hatta gerçek kişiye ait olup olmaması bakımından bir ayrım yapılmamasının suçla mücadele açısından bir eksiklik oluşturduğu düşünüldüğünden kamu kurumlarının bilişim sistemlerine gerçekleştirilen hukuka aykırı girme veya kalma fiilinin cezayı artıran nitelikli hal olarak düzenlenmesi uygun olacağı bunun yanında nesnelerin interneti teknolojisi ve 5G ile birlikte birbirine bağlı çok fazla cihazın bulunacak olması, bilişim ağlarının büyümesiyle de bilişim suçlarının da çeşitlilik kazanacağı önümüzdeki günlerde klasik anlamdaki suçların birçoğunun bilişim sistemlerinin araç olarak kullanılması suretiyle gerçekleştirilebilmesinin mümkün hale gelebileceği göz önüne alındığında öngörülü bir düzenleme ile bilişim sistemlerinin araç olarak kullanılmasının sadece hırsızlık ve dolandırıcılık suçuna hasredilmesinin yetersiz kalacağı, öncelikle bilişim alanında suç tipine haiz olan 243. ve 244. m.' lerde yer alan suçların tek bir madde içerisinde farklı fıkralar olarak bir bütün halinde düzenlenmesinin, bu madde içerisinde ise diğer herhangi klasik suç tipi açısından bilişim sistemlerinin araç olarak kullanılmasının genel ağırlaştırıcı sebep olarak kabul edilmesinin yerinde bir düzenleme olacağı değerlendirilmektedir.

TCK' nın 243. m.' sinin 4. fıkrasında yer alan veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçunun düzenlenmiş olduğu yerin madde başlığı ile uyumlu olmaması sebebiyle 245/A m.' sinde olduğu gibi 243/A şeklinde (veya birleştirilecek madde numarasına göre) düzenlenmesinin yasa yapma tekniği açısından uygun olacağı değerlendirilmektedir.

TCK' nın 244. m.' sinin 2. fıkrasında yer alan suç tipi, her ne kadar kanunkoyucu tarafından boşluk bırakmamak adına düzenlemişse de "verileri başka bir yere gönderme" fiilinin bir belirsizlik oluşturması sebebiyle yeniden değerlendirilmesi gerektiğini düşünmekteyiz.

TCK' nın 244. m.' sinin 3. fıkrasında, her ne kadar toplumun büyük bir kısmını etkileyecek ve hatta zarar verebilecek bir halin dikkate alınarak nitelikli bir hal düzenlenmesi yerinde ise de siber terör başlığı altında da belirtmiş olduğumuz üzere ülkenin kritik altyapılarına yönelmiş saldırıların (veya maddede belirtilen fiillerin) ayrıca dikkate alınarak düzenleme yapılmasında fayda görülmektedir. Nitekim, kritik

altyapı olarak belirlenen hizmetler sadece kamusal tarafta yürütülen bir hizmet niteliği taşımamaktadır. Bu bağlamda ilgili başlık altında da belirtmiş olduğumuz üzere bu m.' ye 244/A şeklinde (veya birleştirilecek olan madde numarasına göre) bir madde eklenilmek suretiyle kritik altyapılara yönelik fiillerin kamu veya özel sektör ayrımı yapılmaksızın bir bütün olarak hizmetin korunması anlamında ayrıca düzenleme altına alınması gerektiğini değerlendirmekle birlikte doktrinde belirtilmiş olan var olan 3. fıkra düzenlemesine bu kurumlarda çalışan görevlilerin sahip oldukları imkanların kolaylığından faydalanmak suretiyle işlenmesi halinin eklenmesi bunun yanında maddede düzenlenen cezai yaptırım hususunda ise alt ve üst sınır belirlenmesinin daha yerinde bir düzenleme olacağı fikrine katılmaktayız.

TCK' nın 245. m.' sinde düzenlenen banka veya kredi kartlarının kötüye kullanılması suçlarının esasen hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının banka veya kredi kartlarının kullanılarak işlendiği şekilleri olarak bağımsız ve kendine özgü bir norm olarak düzenlenmiş hali olarak kabul ettiğimiz ve 245. m. düzenlemesinin tümü itibariyle düzenlemesinde bilişim sistemlerinin araç olarak kullanıldığı ancak öncelikli olarak malvarlığı değerlerini koruduğunu düşündüğümüz için "bilişim alanında suçlar" bölümünde düzenlenmesinin isabetli olmadığı, malvarlığına karşı suçlar bölümünde düzenlenmesinin daha uygun olacağını değerlendirmekteyiz.

TCK' nın 245/A m.' sinde yer alan "Yasak cihaz veya programlar" suç tipinin ise madde başlığının eylem unsurunu ön plana çıkaracak şekilde yeniden düzenlenmesi gerektiği değerlendirilmektedir.

Son olarak suçla etkin mücadelenin sağlanabilmesinin, etkin cezai yaptırımları da içermesi gerektiği düşüncesi ile bilişim teknolojilerinin ve bilişim sistemlerinin hayatımızda edindiği yer ile bu alanda gerçekleştirilecek ihlallerin etkisinin de göz önünde bulundurulması suretiyle "bilişim alanında suçlar" bölümünde yer alan suçlar için düzenlenen hapis cezalarının alt ve üst sınırlarının yeniden değerlendirilerek arttırılması gerektiği değerlendirilmektedir.

KAYNAKÇA

Akbulut Bozdoğan Berrin (2000), "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, Milenyum Armağanı, Sayı: 1-2, C: 8, Konya.

Akbulut Berrin (2017), *Bilişim Alanında Suçlar*, Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Adalet Yayınevi, Ankara.

Akolaş D. Arzu, "Bilişim Sistemleri ve Bilişim Teknolojisini Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları", http://dergisosyalbil.selcuk.edu.tr/susbed/article/view/693/645, ET. 27 Ocak 2020.

Akpek Nusret Onur (2015), *Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Aliusta Cahit, Benzer Recep, (2018), "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* Cilt:4, No:2, ss. 35-42.

Alkan Mustafa (2019), " 'Kuantum Sonrası Kriptoloji' kavramı hayatımıza girdi", 16.07.2019, https://www.bilgiguvenligi.org.tr/kuantum-sonrasi-kriptoloji-kavrami-hayatimiza-girdi/, ET. 24 Ekim 2019.

Alp Barış Emre (2018), *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu*, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

ANADOLU AJANSI, "USOM'a idari para cezası kesme yetkisi verildi", Anadolu Ajansı, 30.09.2018, https://www.aa.com.tr/tr/turkiye/usoma-idari-para-cezasi-kesme-yetkisi-verildi-/1268694, ET. 26 Ekim 2019.

Apaydın Cengiz (2016), "Bilişim Sistemine Girme Suçu", *Türkiye Adalet Akademisi Dergisi,* Yıl: 7, Sayı: 24, Ocak 2016, ss. 245- 306.

Apaydın Cengiz (2015), "Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları", *Ceza Hukuk Dergisi,* Yıl: 10, Sayı: 29, Aralık 2015, ss. 205-263.Arıcı Haydar Yener (2018), *Adli Bilişim : Kavram – Bilgiler - Uygulama Adli Bilişimde Müdahale ve Sonraki Süreçler*, 1. Baskı, Seçkin Yayıncılık, Ankara.

Artuk Mehmet Emin, Gökcen Ahmet, Yenidünya A. Caner (2007), *5237 Sayılı Kanuna Göre Hazırlanmış Ceza Hukuku Özel Hükümler*, 8. Bası, Turhan Kitabevi Yayınları, Ankara.

Artuk Mehmet Emin, Gökcen Ahmet, Yenidünya A. Caner (2014), *Türk Ceza Kanunu Şerhi: Madde 234-345,* Cilt:V, Genişletilmiş ve Yargıtay Kararlarıyla Zenginleştirilmiş 2. Baskı, Adalet Yayınevi, Ankara.

AVRUPA BİRLİĞİ TÜRKİYE DELEGASYONU, "AB Türkiye'de Şebeke ve Bilgi Sistemleri Güvenliğini Destekliyor", 11.04.2019, https://www.avrupa.info.tr/tr/pr/ab-turkiyede-sebeke-ve-bilgi-sistemleri-guvenligini-destekliyor-9420, ET. 20 Mart 2020.

Aydın Emin Doğan (Aralık 1992), "Bilişim Sistemlerinde Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları", *Marmara İletişim Dergisi,* Sayı: 1, ss. 109-137, https://dergipark.org.tr/tr/download/article-file/2664, ET. 16 Mart 2020.

Aydın Emin Doğan (1992), *Bilişim Suçları ve Hukukuna Giriş*, 1. Baskı., Doruk Yayınları, Ankara.

Aydın Emin Doğan (1999), *Telsim'in katkılarıyla Bilişim ve Telekomünikasyon Terimler Sözlüğü*, Telsim Yayınları-1, Ankara, Ağustos 1999.

BASIN İLAN KURUMU, "Dünya 6 trilyon dolarlık siber saldırı riskine karşı hazırlanıyor", Editör: Mavlüt Çiftçi, 15.03.2019, https://www.bik.gov.tr/dunya-6trilyon-dolarlik-siber-saldiri-riskine-karsi-hazirlaniyor/, ET. 18 Şubat 2020.

BASIN İLAN KURUMU, "Nato siber savunmaya odaklanıyor", (2019), Editör: Mevlüt Çiftçi, 30.08.2019, https://www.bik.gov.tr/nato-siber-savunmaya-odaklaniyor/, ET. 15 Şubat 2020.

BASIN İLAN KURUMU, "Teknolojiyle kapıyı çalan tehlike: Siber Saldırı" Editör: Ömer Faruk Orkçu, 16. 03.2019, https://www.bik.gov.tr/teknolojiyle-kapiyi-calan-tehlike-siber-saldiri/, ET. 18 Şubat 2020.

Başaran Alper (2016), *Siber Savaş Cephesinden Notlar*, Arıon Yayınevi, İstanbul.

Bensghir Kaya Türksel (2002), "Türkiye' de Yönetim Bilişim Sistemleri Disiplinin Gelişimi Üzerine Düşünceler", *Amme İdaresi Dergisi,* Cilt: 35, Sayı:1, ss. 77-103.

Berber Keser Leyla (2008), "Adli Bilişim, CMK md. 134 ve Düşündürdükleri…", 10.07.2008, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html, ET. 26 Ekim 2019.

Bıçak Vahit (2007), *Mukayeseli-Gerekçeli Türkçe- İngilizce Türk Ceza Kanunu*, 2. Bası, Seçkin Yayınevi, Ankara.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, "Bakan Yardımcısı Sayan: Günümüzün En Önemli Konusu Dijital Ekonomi", 5.02.2020, https://www.btk.gov.tr/haberler/bakan-yardimcisi-sayan-gunumuzun-en-onemli-konusu-dijital-ekonomi, ET. 22 Şubat 2020.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, "Kablosuz Ağların Geleceği ve 5G'nin Önemi Konuşuldu", 30.10.2019, https://www.btk.gov.tr/haberler/kablosuz-aglarin-gelecegi-ve-5g-nin-onemi-konusuldu, ET. 23 Mart 2020.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, "Siber Kalkan 2019 Sona Erdi", 20 Aralık 2019, www.btk.gov.tr/haberler/siber-kalkan-2019-sona-erdi, ET. 18 Şubat 2020.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, "2020-2023 Siber Güvenlik Stratejileri BTK'da Belirlendi", 10.02.2020, https://www.btk.gov.tr/haberler/2020-2023-siber-guvenlik-stratejileri-btk-da-belirlendi, ET. 20 Şubat 2020.

"Bilgisayar Donanım Notları", http://w3.gazi.edu.tr/~iguler/ebe250/bilg_donanim.pdf, ET. 13 Ekim 2019.

"Bilgisayar Donanımı", http://web.bilecik.edu.tr/bulent-turan/files/2012/10/donanim.pdf, ET. 13 Ekim 2019.

"Bilgisayara Giriş", http://kisi.deu.edu.tr/huseyin.avunduk/bilgisayara_giris.pdf, ET. 12 Ekim 2019.

"Bilgisayara Giriş Ders Notları", http://web.iku.edu.tr/~tkaynas/bgdn2.pdF, ET. 12 Ekim 2019.

"Bilişim Teknolojileri İşletim Sitemi Temelleri", (2007), T.C. Milli Eğitim Bakanlığı MEGEP (Meslekî Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi), Ankara, 2007, https://www.ismek.ist/files/ismekOrg/file/2013_hbo_program_modulleri/isletimsistemleritemeller.pdf, ET. 13 Ekim 2019.

Bilişim Terimleri Sözlüğü İngilizce-Türkçe, (2006), Hazırlayanlar: Ali Arifoğlu, Mehmet Demirer, Gökhan Şengül, Osman Öz, 1. Basım, Türk Standartları Enstitüsü, Onur Matbaacılık, İstanbul, Mayıs.

Bük Alaattin (2018), *Bilişim Alanında Kişisel Verilerin Korunması*, Seçkin Yayıncılık, Ankara.

Can Hayrettin, Akın Erhan (2006), "Akıllı Ev Aygıtları", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss. 73-78.

Cılız Kemal (2006), "Bilişim Teknolojisinde Gelişmeler", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss. 246-248.

Civiloğlu Ahu Sinem, Tanyeri Gizem, (2007), "Bilişim Suçları ve Çocuk Pornografisi", *Hukuk Gündemi Dergisi,* Sayı: 7, Bahar 2007, ss. 95-101.

CNNTURK, "Ahtapot yazılımı nedir, nerede kullanılıyor?" 22.12.2018 https://www.cnnturk.com/video/bilim-teknoloji/teknoloji/ahtapot-yazilimi-nedir-nerede-kullaniliyor, ET. 27 Ekim 2019.

CNNTURK, "WannaCry saldırısının ardında yatan gerçekler", 16.05.2017, https://www.cnnturk.com/teknoloji/wannacry-saldirisinin-ardinda-yatan-gercekler, ET. 9 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cdpc, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/capacity-building-programmes, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/web/cybercrime/cybercrime-office-c-proc-, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/cybereast, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/cybersouth, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/endocsea-europe, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/glacyplus, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/cybercrime-octopus, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/tcy, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/iproceeds-2, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/t-cy-drafting-group, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/t-cy-reports, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/the-budapest-convention, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/effectiveness-of-the-mutual-legal-assistance-and-cyberviolence-in-the-focus-of-the-18th-plenary-of-the-t-cy, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/jurisdiction-in-cyberspace-amsterdam-conference-concludes, ET. 1 Mart 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/the-budapest-convention-at-iscr-2018, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/turkey-signed-the-protocol-on-racism-and-xenophobia, ET. 29 Şubat 2020.

COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/-/17th-anniversary-of-the-budapest-convention, ET. 29 Şubat 2020.

CYBERMAG, "Anubis Truva Atından Türkiye'ye Yoğun Saldırı", Sayı: 44, Eylül 2019, ss. 40-41.

CYBERMAG, "Artık Milyonlarca Kişinin Değil, Milyonlarca Doların Peşine Düşüyorlar", Sayı: 36, Ocak 2019, ss. 30-31.

CYBERMAG, "CISCO Orta Doğu ve Afrika Siber Güvenlik Direktörü Fady Younes İle Söyleşi", Sayı: 45, Ekim, 2019, ss. 6-15.

CYBERMAG, "Finansal Hizmetler Sektörü Siber Suçluların Radarında", Sayı: 45, Ekim 2019, ss. 24-27.

CYBERMAG, "Firmalar En Az Bir Kez Ciddi Bir Siber Saldırıya Maruz Kalıyor", Sayı: 34, Kasım 2018, ss. 26-27.

CYBERMAG, "Her 10 Zararlı Yazılımdan Biri Kripto Para Madencisi", Sayı: 34, Kasım 2018, ss. 30-31, s. 30.

CYBERMAG, "HUAWEI'den Yapay Zekalı Firewall Güvenlik Duvarı", 11.11.2018, https://www.cybermagonline.com/huaweiden-yapay-zekali-firewall-guvenlik-duvari, ET. 24 Ekim 2019.

CYBERMAG, "IOT CİHAZLAR İÇİN YETERLİ GÜVENLİK ÖNLEMİ ALINMIYOR!", 16.11.2018, https://www.cybermagonline.com/iot-cihazlar-icin-yeterli-guvenlik-onlemi-alinmiyor, ET. 22 Ekim 2019.

CYBERMAG, "IOT CİHAZLAR KİŞİSEL VERİ GÜVENLİĞİNİ TEHDİT EDİYOR", 28.09.2018, https://www.cybermagonline.com/iot-cihazlar-kisisel-veri-guvenligini-tehdit-ediyor, ET. 23 Ekim 2019.

CYBERMAG, (2019), "Kuantum Bilgisayarlar Siber Saldırganların Eline Geçerse Ne Olur?", Temmuz 2019, Bilgi Güvenliği Derneği, Sayı: 42.

CYBERMAG, "Privia Security Ağustos Ayı Siber Güvenlik Gelişmeleri Bülteni", Sayı: 44, Eylül 2019, ss. 30-33, s. 32.

CYBERMAG, "Siber Saldırganlar Yakalanmamak İçin Atlatma ve Anti Analiz Tekniklerine Yöneliyor", Sayı: 45, Ekim, 2019, ss. 26-27.

CYBERMAG, "Siber Tehditlerin Yeni Silahı: Sosyal Medya", Sayı: 45, Ekim 2019, ss. 34-35.

CYBERMAG, "Son 10 Yılda 190 Milyon Sağlık Kuruluşu Verisi İfşa Edildi", Sayı: 45, Ekim, 2019, ss. 38-39.

CYBERMAG, "Türkiye, Orta Doğu'da Siber Saldırıların Odağında", Sayı: 34, Kasım 2018, s. 33.

CYBERMAG, "WannaCry 2018'in 3. Çeyreğinde Yaklaşık 75.000 Kullanıcıyı Etkiledi", Sayı: 36, Ocak 2019, ss. 42-43.

CYBERMAG, "WhatsApp Üzerinden Telefonlara Casus Yazılım Yerleştirildi", Sayı: 42, Temmuz 2019.

CYBERMAG, "12. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", 16.10.2019, https://www.cybermagonline.com/12-uluslararasi-bilgi-guvenligi-ve-kriptoloji-konferansi, ET. 23 Ekim 2019.

CYBERMAG, "2018'in Siber Tehditlerini Tanımlayan Kelimeler: Gizli ve Daha Zeki", Sayı: 34, Kasım 2018, ss. 24-25.Çakıcı Mert (Nisan 2014), "Türk Ceza Kanunu M.243 ve M.244' te Düzenlenen Bilişim Suçları", *Ceza Hukuk Dergisi*, Yıl: 9, Sayı: 24, ss. 307-349.

CYBERMAG, "2019'un Siber Tehditleri İşletmeleri Yeni Önlemler Almaya Zorlayacak", 13.11.2018, https://www.cybermagonline.com/2019un-siber-tehditleri-isletmeleri-yeni-onlemler-almaya-zorlayacak, ET. 23 Ekim 2019.

Çakmak Haydar, Demir Cenker Korhan (2009), *Suç, Terör & Savaş Üçgeninde Siber Dünya*, "Siber Dünyadaki Tehdit ve Kavramlar", Editörler: Haydar Çakmak, Taner Altunok, Barış Platin Kitabevi, Ankara, ss.23-55.

Çelik Soner (2018), "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *Academic Review of Humanities and Social Sicences*, Vol.:1, Issue:2, pp. 110-119.

Çiftçi Hasan (2017), *Her Yönüyle Siber Savaş*, Güncellenmiş ve genişletilmiş 2. Basım, Tübitak Popüler Bilim Kitapları, Salmat Basım Yayımcılık, Ankara.

Çölkesen Rifat (2006) "Veri Yapıları ve Modelleri", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss. 892-897.

Dağ Funda (2006), "Yapay Zekâ: Temel Kavramlar", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss.935-939.

Darıcılı Ali Burak (2017), *Siber Uzay ve Siber Güvenlik Nedir? (ABD' nin Siber Güvenlik Stratejisi Rusya Federasyonu' nun Siber Güvenlik Stratejisi)*, Dora Basım-Yayın, Bursa.

Değirmenci Olgun (2002), *Bilişim Suçları*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Değirmenci Olgun (2003), "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", *Legal Hukuk Dergisi,* Cilt:1, Sayı: 11, ss. 2750-2758.

Değirmenci Olgun (2005), "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", *Türkiye Barolar Birliği Dergisi,* Sayı: 58, Yıl: 18, Mayıs-Haziran 2005, ss. 195-208.

Demir Ceren (2019), "IBM, Kuantum Bilgisayarlarını En Geç 5 Yıl İçinde Piyasaya Sürmeye Hazırlanıyor", 31.05.2019, http://inovasyon101.com/kuantum-bilgisayar-ibm/, ET. 18 Ekim 2019.

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

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

Doğan Ramazan (2014), *5237 Sayılı Türk Ceza Kanunu' nda Bilişim Suçları,* Adalet Yayınevi, Ankara.

Doğru Ali Haydar (2017), *Bilişim Hukuku : Bilgi ve İletişim*, Gözden Geçirilmiş 2. Baskı, Ekin Yayınevi, Bursa.

Dursun Hasan (1998), "Bilgisayar İle İlgili Suçlar", *Yargıtay Dergisi*, Sayı: 1-2, Ocak-Nisan 1998, ss. 334-339.

Dülger Murat Volkan (2004), *Bilişim Suçları*, Seçkin Yayınevi, Ankara.

Dülger Murat Volkan (Temmuz 2017), "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", *Türkiye Adalet Akademisi Dergisi,* Sayı:31, Yıl:8, ss. 141-256.

Dülger Murat Volkan (2018), *Bilişim Suçları ve İnternet İletişim Hukuku*, Tamamen Güncellenmiş 7. Baskı, Seçkin Yayınevi, Ankara.

Dülger Murat Volkan, Modoğlu Gözde (t.y.), *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet İletişim Hukuku (Uygulama Rehberi)*, Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği/Avrupa Konseyi Ortak Programı, y.y.

Dülger Murat Volkan, Modoğlu Gözde, (t.y.), *Bilişim Suçları Eğitim Modülü*, Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği/Avrupa Konseyi Ortak Programı, y.y.

Eczacıbaşı Faruk (2016), *"Siber Risklerin Yönetimi*, "1. Oturum Dünya ve Türkiye'deki Siber Tehditler ve Hayatımıza Etkileri", *Risk Management Forum* 2015, Nart Sigorta ve Reasürans Brokerliği A.Ş., 1. Baskı, İstanbul, ss. 25-27.

Efe Ali, Çölkesen Rifat (2006), "Ağ Programlama ve TCP/IP", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss. 55-60.

Eker Ö. Umut, (2006), " '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,* Yıl: 19, Sayı: 62, Ocak-Şubat 2006, ss. 101-131.

Emmungil, Levent, (2010), *Bilgisayar Donanımı*, Ankara, E-Kitap, http://it.famergroup.com/bilgisayardonanim.pdf, ET. 13 Ekim 2019.

Epözdemir Rezan, (Haziran 2018), "Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri", *Terazi Aylık Hukuk Dergisi*, Bilişim Hukuku Özel Sayısı, Cilt: 13, Sayı: 142, ss. 88-98.

Ercan Tuncay, Kutay Mahir (2016), "Endüstride Nesnelerin Interneti (IoT) Uygulamaları", *Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi,* ss. 509-607, https://fenbildergi.aku.edu.tr/wp-content/uploads/2016/12/035102-599-607.pdf, ET. 19 Ekim 2019.

Erdağ Ali İhsan, (2010), "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: XIV, Sayı: 2, Yıl: 2010, ss. 275-303, http://webftp.gazi.edu.tr/hukuk/dergi/14_2_10.pdf, ET. 5 Mart 2020.

Erdoğan Yavuz (2012), "Bilişim Sistemine Girme ve Kalma Suçu", Prof. Dr. Burhan Ceyhan'a Armağan II, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* Cilt: 12, Özel Sayı, Yıl: 2010, İzmir, ss. 1363-1432.

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

Erdoğan Yavuz (2018), *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* Legal Yayıncılık, İstanbul.

Ergün İsmail (2008), *Siber Suçların Cezalandırılması ve Türkiye' de Durum*, 1. Baskı, Adalet Yayınevi, Ankara.

Ersoy Yüksel (1994), "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", *Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi*, Cilt:49, Sayı:3-4, Ankara, ss. 149-183, https://dspace.ankara.edu.tr/xmlui/bitstream/handle/20.500.12575/52267/5320.pdf?sequence=1&isAllowed=y, ET. 1 Nisan 2020.

Eryaman Damla (2018), *Türk Ceza Kanunu'nda Bilişim Suçları*, Çağ Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, Mersin, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

EUROPOL, https://www.europol.europa.eu/about-europol, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf, ET. 1 Mart 2020.

EUROPOL, "CYBERCRIME", https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/events/6th-interpol-europol-cybercrime-conference, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/iocta/2017/THE_GEOGRAPHIC_DISTRIBUTION_OF_CYBERCRIME.html, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/newsroom/news/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/newsroom/news/media-invitation-to-opening-of-european-cybercrime-centre-ec3-europol, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/newsroom/news/setting-scene-for-cybercrime-trends-and-new-challenges, ET.1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/newsroom/news/5th-europol-interpol-cybercrime-conference-successfully-ends-record-participation-and-concrete-steps-for-future, ET. 1 Mart 2020.

EUROPOL, https://www.europol.europa.eu/newsroom/news/60-e-commerce-fraudsters-busted-during-international-operation, ET. 1 Mart 2020.

EUROPOL, "THE HIDDEN RISKS OF SOCIAL MEDIA", Europol, 5.01.2011, https://www.europol.europa.eu/newsroom/news/hidden-risks-of-social-media, ET. 1 Mart 2020.

EUROJUST, http://www.eurojust.europa.eu/Practitioners/Data-Protection/Pages/Data-protection-at-Eurojust.aspx, ET. 1 Mart 2020.

EUROJUST, http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx, ET. 1 Mart 2020.

EUROJUST, http://www.eurojust.europa.eu/press/News/News/Pages/2019/2019-11-15_EJCN-7th-plenary.aspx, ET. 1 Mart 2020.

EUROJUST, http://www.eurojust.europa.eu/press/News/News/Pages/2020/2020-01-28_Cybercrime-Judicial-Monitor-Issue5.aspx, ET. 1 Mart 2020.

Gerçek Alper, Gökşen Haluk, (t.y.), *Kobiler İçin Dijital Dönüşüm Rehberi Endüstri 4.0,* Türkiye Bilişim Derneği, Ankara Ofset, Ankara.

Gökçöl Orhan, Yavuzer Selvihan Nazlı (2006), "İnternet Adresleri, IP ve DNS", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss. 455-462.

Gözü Ömer, Aydın Selçuk Han (2009), *Temel Bilgisayar Kullanımı*, Editörler Hasan Nadir Derin, Feride Erdal, Sürüm 3, Orta Doğu Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı, Aralık 2009, http://file.cc.metu.edu.tr/ccweb/bidb_ccusg/TBK2009pub.pdf, ET. 12 Ekim 2019.

Gözüşirin Mesih (2011), *5237 sayılı Türk Ceza Kanunu'nda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi*, Kara Harp Okulu Savunma Bilimleri

Enstitüsü Güvenlik Bilimleri Anabilim Dalı Yüksek Lisans Tezi, Ankara, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Gül Ahmet (2018), *Doğrudan/Dolaylı Bilişim Suçları*, Genişletilmiş ve Güncellenmiş 2. Baskı, Seçkin Yayınevi, Ankara.

Gürler Fazlı (2013), *Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar*, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Yüksek Lisans Tezi, Ankara, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

Güneş Alper (2015), *Bilişim Suçları ve İdarenin Hukuki Sorumluluğu*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, Yüksek Lisans Tezi, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Gürkaynak Muharrem, İren Adem Ali (2011), "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, S:2, C:16, ss. 263-279.

HABERTÜRK, "IPv6'ya geçiş başladı!", 24.06.2012, https://www.haberturk.com/ekonomi/teknoloji/haber/715819-ipv6ya-gecis-basladi, ET. 31 Ekim 2019.

Harmancı A. Emre (2006), "Ağ Mimarisi", *Türkiye Bilişim Ansiklopedisi,* Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss. 49-55.

H.C. Mult. Ulrich Sieber (2014), *İnternetteki Suçlar ve Suçun İnternette Takibi : Global Bilgi Toplumundaki Yeni Gelişmelerin Işığında Hangi Önlemler Tavsiye Edilmektedir?*, Editör: Yener Ünver, Çeviren: Yener Ünver, Mustafa Temmuz Oğlakcıoğlu, Seçkin Yayıncılık, Ankara.

Hekim Hakan, Başıbüyük Oğuzhan (2013), "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, 4 (2), ss. 135-158.

https://afyonluoglu.org/siberguvenlik/nist-reports/, ET. 3 Mart 2020.

https://legalbank.net/arama

https://www.hukukmedeniyeti.org/ictihat/877255/, ET. 15 Temmuz 2020.

https://www.hukukmedeniyeti.org/karar/2789451/, ET. 15 Temmuz 2020.

https://www.hukukmedeniyeti.org/karar/2161414/yargitay-5-ceza-dairesi-e-2014-6872-k-2014-7366/, ET. 15 Temmuz 2020.

https://www.lexpera.com.tr/, ET. 15 Temmuz 2020.

https://www.mevzuat.gov.tr/, ET. 14 Temmuz 2020.

https://resmigazete.gov.tr/eskiler/2011/09/20110920-4.htm, ET. 1 Nisan 2020.

https://sozluk.gov.tr/, ET. 19 Mart 2020.

http://tdk.org.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5d9a02a3991702.19216647, ET. 6 Ekim 2019.

https://tr.wikipedia.org/wiki/Avrupa_Konseyi, ET. 29 Şubat 2020.

https://tr.wikipedia.org/wiki/Birleşmiş_Milletler_Uyuşturucu_ve_Suç_Ofisi, ET. 28 Şubat 2020.

https://tr.m.wikipedia.org/wiki/Denial-of-service_attack, ET. 20 Şubat 2010.
https://tr.m.wikipedia.org/wiki/GCHQ, ET. 20 Şubat 2020.

https://tr.m.wikipedia.org/wiki/Gelişmiş_Sürekli_Tehdit, ET. 20 Şubat 2020.

https://tr.wikipedia.org/wiki/G8, ET. 29 Şubat 2020.

https://tr.wikipedia.org/wiki/Interpol, ET. 2 Mart 2020.

https://tr.wikipedia.org/wiki/OECD, ET. 29 Şubat 2020.

https://www.nsf.gov/about/, ET. 29 Ekim 2019.

https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/, ET. 27 Ekim 2019.

HÜRRİYET, "Kuantum bilgisayarlar siber güvenlikte neleri değiştirecek", (2019), 13.05.2019, http://www.hurriyet.com.tr/teknoloji/kuantum-bilgisayarlar-siber-guvenlikte-neleri-degistirecek-41211945, ET. 18 Ekim 2019.

HÜRRİYET, "Kuantum Bilgisayarlar ve Kübitler"; "Kuantum bilgisayarlar siber güvenlikte neleri değiştirecek", Hürriyetcom.tr, 13.05.2019, http://www.hurriyet.com.tr/teknoloji/kuantum-bilgisayarlar-siber-guvenlikte-neleri-degistirecek-41211945, ET. 18 Ekim 2019.

HÜRRİYET, "Siber savaşlara "yerli ve milli hazırlık", 25.09.2019, http://www.hurriyet.com.tr/teknoloji/siber-savaslara-yerli-ve-milli-hazirlik-41337621, ET. 26 Ekim 2019.

HÜRRİYET, "Yapay zeka nedir? Yapay zeka ne demek?" Hürriyetcom.tr, 6.07.2018, http://www.hurriyet.com.tr/teknoloji/yapay-zeka-nedir-yapay-zeka-ne-demek-40888243, ET. 18 Ekim 2019.

İçel Kayıhan, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana ilkeleri" ", https://docplayer.biz.tr/33880825-Avrupa-konseyi-siber-suc-sozlesmesi-baglaminda-avrupa-siber-suc-politikasinin-ana-ilkeleri.html, ET. 1 Mart 2020.

İnan Ahmet Tevfik (2006), "Ağ Standartları", *Türkiye Bilişim Ansiklopedisi,* Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss. 61-67.

İnce Fuat (2006), "Bilgi Güvenliği", *Türkiye Bilişim Ansiklopedisi,* Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1. Basım, Türkiye Bilişim Vakfı, İstanbul, Papatya Yayıncılık, ss. 162-166.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/about/Pages/default.aspx, ET. 26 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx, ET. 28 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/action/cybersecurity/Pages/itu-resolutions.aspx, ET. 27 Şubat 2020.

INTERNATIONAL COMMUNICATION UNION, https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx, ET. 27 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/action/Pages/default.aspx, ET. 26 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/en/history/Pages/DiscoverITUsHistory.aspx, ET. 26 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html, ET. 28 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/md/T05-SG17-070919-TD-WP2-2779, ET. 27 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/md/D10-SG01-C-0203, ET. 28 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, https://www.itu.int/md/T13-SG17-C-0340, ET. 27 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, "Cyber Shield 2019" https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/CyberShield/Cyber-Shield-2019.aspx, ET. 24 Şubat 2020.

INTERNATIONAL TELECOMMUNICATION UNION, "Vienna Cyber Security Week 2019", https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/cybervienna.aspx, ET. 25 Şubat 2020.

INTERNATIONAL TELECOMUNICATION UNION, "28 August: ITU workshop on advanced cybersecurity attacks and ransomware", 16.08.2018, https%3a%2f%2fnews.itu.int%2f28-august-itu-workshop-on-advanced-cybersecurity-attacks-and-ransomware%2f, ET. 27 Şubat 2020.

INTERPOL, https://www.interpol.int/Crimes/Cybercrime, ET. 1 Mart 2020.

INTERPOL, https://www.interpol.int/Crimes/Cybercrime/Cyber-partnerships, ET. 3 Mart 2020.

INTERPOL, https://www.interpol.int/Crimes/Cybercrime/Investigative-support-for-cybercrime, ET. 2 Mart 2020.

INTERPOL, https://www.interpol.int/Crimes/Cybercrime/Our-cyber-operations, ET. 2 Mart 2020.

İSTANBUL TEKNİK ÜNİVERSİTESİ, "Bellek Türleri", 6.09.2013, http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/bellek-turleri, ET. 13 Ekim 2019.

İSTANBUL TEKNİK ÜNİVERSİTESİ, "Internet of Thing (IOT)", 15.01.2019, https://bidb.itu.edu.tr/seyir-defteri/blog/2019/01/15/internet-of-thing-(iot), ET. 01 Şubat 2020.

İSTANBUL TEKNİK ÜNİVERSİTESİ, "İnternet'in Tarihçesi", 07.09.2013, https://tercih.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi, ET. 29 Ekim 2019.

İSTANBUL TEKNİK ÜNİVERSİTESİ, "IPSec VPN (Internet Protocol Security – İnternet Protokolü Güvenliği)", 07.09.2013, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ipsec-vpn-(internet-protocol-security-internet-protokol%C3%BC-g%C3%BCvenli%C4%9Fi), ET. 28 Ekim 2019.

İSTANBUL TEKNİK ÜNİVERSİTESİ, "SSL VPN (Secure Sockets Layer Virtual Private Network - Güvenli Yuva Katmanı Tabanlı Sanal Özel Ağ)", 07.09.2013, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ssl-vpn-(secure-sockets-layer-virtual-private-network---g%C3%BCvenli-yuva-katman%C4%B1-tabanl%C4%B1-sanal-%C3%B6zel-a%C4%9F), ET. 28 Ekim 2019.

Kara İlker, Kaya Gamze (t.y.), "Türkiye' de Bilişim Alanında İşlenen Suçların Uygulama Bakımından Hukuki Boyutunun Değerlendirilmesi", *Kazancı Hukuk Araştırmaları Dergisi*, ss. 154- 167.

Kara Mahruze (2013), *Siber Saldırılar- Siber Savaşlar ve Etkileri*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Karagöz Mehmet Can (2019), *Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)*, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Yüksek Lisans Tezi, Antalya, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Karagülmez Ali (2005), *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Genişletilmiş ve Gözden Geçirilmiş 4. Baskı, Seçkin Yayınevi, Ankara.

Karagülmez Ali, (2010), "Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu", *Türkiye Adalet Akademisi Dergisi*, Cilt:1, Yıl:1, Sayı:3, Ekim 2010, ss. 235, 256.

Karakehya Hakan (2009), "Türk Ceza Kanununda Bilişim Sistemine Girme Suçu", *Türkiye Barolar Birliği Dergisi,* Yıl: 22, Sayı: 81, Mart-Nisan 2009, ss. 1-24.

Kaya Mehmet Bedii (2019), "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik, Adli Bilişim ve Güncel Teknolojiler"*, Siber Güvenlik ve Savunma : Problemler ve Çözümler*, Editörler: Şeref Sağıroğlu, Mustafa Şenol, BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Grafiker Yayınları, Ankara, ss. 213-269.

Keser Berber Leyla (2004), *Adli Bilişim (Computer Forensic),* Yetkin Yayınları, Ankara.

Ketizmen Muammer (2006), *Türk Ceza Hukukunda Bilişim Suçları*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Doktora Tezi, Ankara, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Ketizmen Muammer (2008), *Türk Ceza Hukukunda Bilişim Suçları*, y.y., Adalet Yayınevi.

Kılan Kaya N. (2006), "Algoritma ve Harzemli (Al-Harezmi) Musa Oğlu Muhammed", *Türkiye Bilişim Ansiklopedisi,* Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1.Basım, Türkiye Bilişim Vakfı, Papatya Yayıncılık, İstanbul, ss. 84-86.

Kızıltan Mehmet Burak (2007), *5237 sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

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

Köprülü Tacettin (2019), "Cumhurbaşkanlığı "Bilgi ve İletişim Güvenliği Tedbirleri" Genelgesi' ne İlişkin Değerlendirme", *CyberMag*, Sayı: 44, Eylül 2019.

Kul Haluk (2009), *İşletmeciler İçin Bilişim Sistemleri Temelleri ve Uygulamaları*, 1. Basım, Papatya Yayıncılık, İstanbul.

Kurt Levent (2005), *Açıklamalı- İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Seçkin Yayıncılık, Ankara.

Laudon Kenneth C., Laudon Jane P. (2011), *Yönetim Bilişim Sistemleri (Dijital İşletmeyi Yönetme),* Çeviri Editörü: Uğur Yozgat, Çevirenler: Adem Öğüt, Vahap Tecim, Tunçhan Cura, Ayşe Yıldız, F. Oben Ürü, Fehmi Volkan Akyön, İbrahim Edin, İlknur Kumkale, Özlem Oktal, Ömür Yaşar Saatçıoğlu, Nihal Kartaltepe Behram, 12. Basımdan Çeviri, Nobel Akademik Yayıncılık, Ankara.

Levi Albert (2006), "Ağ Güvenliği", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1.Basım, Türkiye Bilişim Vakfı, Papatya Yayıncılık, İstanbul, ss. 44-49.

Longman Dictionary of English Language and Culture, (1998), Second edition, Addison Wesley Longman Limited Edinburgh Gate, England.

Mahmutoğlu Fatih Selami (2013), "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt: LXXI, Sayı:1, ss. 855-888.

Malkoç İsmail (2008), *Açıklamalı-İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu (Madde 179-345)*, Cilt: II, Geliştirilmiş 3. Baskı, Malkoç Kitabevi, Ankara.

MİLLİYET, "Türkiye'ye siber saldırı şoku: Kaynağı ABD ve Rusya!", Milliyet, 30.10.2019, https://www.milliyet.com.tr/teknoloji/turkiyeye-siber-saldiri-soku-kaynagi-abd-ve-rusya-6066357, ET. 9 Şubat 2020.

Muslu Fatih (2006), "Web: html ve http", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1.Basım, Türkiye Bilişim Vakfı, Papatya Yayıncılık, İstanbul, ss. 917-919.

Nacar Fatma Burcu (2010), *Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları*, Atılım Üniversitesi Sosyal Bilimler Enstitüsü Avrupa Birliği Anabilim Dalı Yüksek Lisans Tezi, Ankara, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Ocak Mahir E. (2019), "Kuantum Bilgisayarlar ve Kübitler", 25.03.2019, http://bilimgenc.tubitak.gov.tr/makale/kuantum-bilgisayarlar-ve-kubitler, ET. 18 Ekim 2019.

ODTÜ, http://cisn.odtu.edu.tr/2009-16/vpn.php, ET. 27 Ekim 2019.

OECD, https://www.oecd-ilibrary.org/, ET. 29 Şubat 2020.

OECD, https://www.oecd-ilibrary.org/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en, ET. 29 Şubat 2020.

OECD, https://www.oecd-ilibrary.org/science-and-technology/online-identity-theft/the-scope-of-online-identity-theft_9789264056596-3-en, ET. 29 Şubat 2020.

OECD, https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm, ET. 29 Şubat 2020.

OECD, https://www.oecd.org/sti/ieconomy/32493366.PDF, ET. 29 Şubat 2020.

Orta Mesut (2015), *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)*, Yetkin Yayınları, Ankara.

Orta Mesut (2015), *Bilişim Suçlarında Adlî Analiz*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Konya, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

ORTA DOĞU TEKNİK ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI, "Internet Tarihi", http://www.internetarsivi.metu.edu.tr/tarihce.php, ET. 29 Ekim 2019.

ORTA DOĞU TEKNİK ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI, "IPv6 Nedir?", https://ipv6.metu.edu.tr/tr/node/1, ET. 31 Ekim 2019.

Öğün Mehmet Nesip, Kaya Adem, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri*, Yıl: 9, Sayı:18, http://afyonluoglu.org/PublicWebFiles/Reports-TR/Akademi/Makale-2013-Siber%20G%C3%BCvenli%C4%9Fin%20Milli%20G%C3%BCvenlik%20A%C3%A7%C4%B1s%C4%B1ndan%20%C3%96nemi%20ve%20Al%C4%B1nabilecek%20Tedbirler.pdf, ET. 01 Şubat 2020.

Önok Murat, "Avrupa Konseyi Siber Suç Sözleşmesı Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", Prof. Dr. Nur Centel' e Armağan, ss. 1229-1269, http://dosya.marmara.edu.tr/huk/fak%C3%BCltedergisi/nurcentel/muratonok.pdf, ET. 1 Mart 2020.

Özbek Veli Özer (2007), "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 9, Özel Sayı, ss. 1019-1063.

Özbek Veli Özer, Kanbur Mehmet Nihat, Doğan Koray, Bacaksız Pınar, Tepe İlker, (2015), *Türk Ceza Hukuku Özel Hükümler*, Genişletilmiş ve Güncellenmiş 9. Baskı, Seçkin Yayıncılık, Ankara.

Özel Cevat, "Bilişim-İnternet Suçları", https://docplayer.biz.tr/583371-Bilisim-internet-suclari.html, ET. 02 Kasım 2019.

Özen Muharrem, Baştürk İhsan (2011), *Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku*, 1. Baskı, Adalet Yayınevi, Ankara.

Özkışlalı Gizem (2008), *Küreselleşme, İnternet ve Terörizmin Değişen Yüzü: Siber Terörizm*, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı

Yüksek Lisans Tezi, Ankara, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020, ET. 14 Temmuz 2020.

Öztürk Mahmut Sami (Nisan 2018), "Siber Saldırılar, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi", *Muhasebe ve Vergi Uygulamaları Dergisi*, Özel Sayı, ss. 208-232.

Özyılmaz Ahmet Fatih (2014), *Bilişim Sistemleri, Sağlıkta Bilişim Sistemleri ve Performans*, Beykent Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı Hastane ve Sağlık Kurumları Yönetimi Bilimdalı Yüksek Lisans Tezi, İstanbul, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Pallı Hayati (2008), *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Kayseri, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Parlar Ali, Hatipoğlu Muzaffer (2010), *Açıklamalı – Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu (230 – 345 Maddeler)*, 4. Cilt, Seçkin Yayınevi, Ankara.

Peker Bekir (2010), *Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Uluslar Arası İlişkiler Ana Bilim Dalı Yüksek Lisans Tezi, Konya, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

Polat Oğuz, "Çocuk İstismarında Farklı Bir Kavram: Grooming (Siber Uşaklaştırma) ve Türkiye", Şiddeti Önleme ve Rehabilitasyon Derneği - Acıbadem Mehmet Ali Aydınlar Suç ve Şiddetle Mücadele, *Uygulama ve Araştırma Merkezi Basın Özeti,* http://imdat.org/wp-content/uploads/2019/04/Prof.-O%C4%9Fuz-Polat-23-Nisan-Grooming-Rapor.pdf, ET. 10 Mart 2020.

Sağıroğlu Şeref (2018), "Siber Güvenlik ve Savunma, Önem, Tanımlar, Unsurlar ve Önlemler", *Siber Güvenlik ve Savunma : Farkındalık ve Caydırıcılık*, Editörler: Şeref Sağıroğlu, Mustafa Alkan, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, 1. Basım, Grafiker Yayınları, Ankara, ss. 21- 45.

Sağıroğlu Şeref (2019), "Siber Güvenlik ve Ötesi", *Siber Güvenlik ve Savunma : Problemler ve Çözümler,* Ed.: Şeref Sağıroğlu, Mustafa Şenol, BGD Siber Güvenlik ve Savunma Kitap Serisi 2, 1. Basım, Grafiker Yayınları, Ankara, ss. 25-58.

Samet Refik, Aslan Ömer (2018), "Kötü Amaçlı Yazılımlar ve Analizi", *Siber Güvenlik ve Savunma : Farkındalık ve Caydırıcılık***,** Editör: Şeref Sağıroğlu, Mustafa Alkan, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, 1. Basım, Ankara, Grafiker Yayınları, ss. 227-251.

Samur Mehmet Kemal, Saka Osman, "Kampüs Ağında Sanal Özel Ağ Yapılandırması", *Akademik Bilişim'07 - IX. Akademik Bilişim Konferansı Bildirileri* 31 Ocak - 2 Şubat 2007, Kütahya, Dumlupınar Üniversitesi, ss. 267-272, https://ab.org.tr/ab07/kitap/samur_saka_AB07.pdf, ET. 27 Ekim 2019.

Sankur Bülent (2008), *İngilizce-Türkçe Ansiklopedik Bilişim Sözlüğü*, 3. Baskı, Pusula Yayıncılık, İstanbul.

Sarı Onur (2013), *Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar*, Harp Akademileri Stratejik Araştırmalar Enstitüsü Harp/Harekat Hukuku Ana Bilim Dalı Yüksek Lisans Tezi, İstanbul, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Serpen Arda, (2008), "Temel Bilişim Teknolojilerine Giriş", Hacettepe Üniversitesi, Powerpoint Sunum, 7.10.2008, http://yunus.hacettepe.edu.tr/~denizbas/gmu126/DONANIM.pdf, ET. 12 Ekim 2019.

SİBERBÜLTEN, "Yapay Zekâ, Veri Güvenliği ve GDPR", 2.04.2018, https://siberbulten.com/makale-analiz/yapay-zeka-veri-guvenligi-ve-gdpr/, ET. 21 Ekim 2019.

Sokullu-Akıncı Füsun, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi", *İnternet Ortamında Ceza Sorumluluğu konulu panele sunulan bildiri,*

https://docplayer.biz.tr/24679386-Avrupa-konseyi-siber-suc-sozlesmesinde-yer-alan-maddi-ceza-hukukuna-iliskin-duzenlemeler-ve-ozellikle-internette-cocuk-pornografisi.html, ET. 3 Mart 2010.

Soyaslan Doğan (2016), *Ceza Hukuku Özel Hükümler*, Güncelleştirilmiş 11. Baskı, Yetkin Basımevi, Ankara.

Şahin Cumhur, Özgenç İzzet (2005), *Türk Ceza Hukuku Gazi Külliyatı*, Seçkin Yayınevi, Ankara.

Şahin Yunus Emre (2019), "Siber güvenlik uzmanları bu 7 teknolojinin bilgisayar korsanlarının işlerini kolaylaştırdığını söylüyor", 2.10.2019, https://www.gzt.com/bilim-teknoloji/siber-guvenlik-uzmanlari-bu-7-teknolojinin-bilgisayar-korsanlarinin-islerini-kolaylastirdigini-soyluyor-3512558, ET. 24 Ekim 2019.

Şener Selçuk (2006), *Karar Destek ve Üstyönetim Bilişim Sistemleri ve Türkiye'de Bilişim Sektöründe Bir Analiz*, Beykent Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı Yönetim Bilişim Sistemleri Bilim Dalı Yüksek Lisans Tezi, İstanbul, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 13 Temmuz 2020.

Şenol Mustafa, "Türkiye' de Siber Saldırılara Karşı Caydırıcılık", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, S:1-9, Cilt:3, No:2, 2017, https://docplayer.biz.tr/146120164-Turkiye-de-siber-saldirilara-karsi-caydiricilik.html, ET. 9 Şubat 2020.

Tanör Bülent (1990), "Terörle Mücade Kanunu Üzerine Düşünceler", MHB, Sayı: 1-2, Yıl:10, ss. 165-173, https://cdn.istanbul.edu.tr/file/1CD58DF90A/3D3BD99CDB6C4BC2AAA65A1033855C78?, ET. 21 Şubat 2020.

Taşdemir Kubilay (2006), "Türk Ceza Kanunu' nda Bilişim Suçları", *Türkiye Noterler Birliği Hukuk Dergisi*, Sayı: 129, Şubat 2006, ss. 15-28.

Taşkın Şaban Can (2008), *Bilişim Suçları*, 1. Bası, Beta Yayıncılık, İstanbul.

T.C. BİLİM, SANAYİ VE TEKNOLOJİ BAKANLIĞI, "Türkiye Dijital Yol Haritası (2018)" için bkz. https://cdnendustri40.4flyy.com/file/e267e931e0794d50b5e4ba40306cffcb/tsddtyh.pdf, ET. 2 Şubat 2020.

T.C. DIŞİŞLERİ BAKANLIĞI, http://www.mfa.gov.tr/iktisadi-isbirligi_ve-gelisme-teskilati-_oecd_.tr.mfa, ET. 29 Şubat 2020.

T.C. MİLLİ EĞİTİM BAKANLIĞI, "Bilişim Teknolojileri Ağ Temelleri", (2011), Ankara, http://megep.meb.gov.tr/mte_program_modul/moduller_pdf/a%C4%9F%20temelleri.pdf, ET. 27 Ekim 2019.

T.C. ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI, "2016-2019 Ulusal Siber Güvenlik Stratejisi", https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, ET. 2 Şubat 2020.

Türk Dil Kurumu Türkçe Sözlük, (1998), Hazırlayanlar: İsmail Parlatır, Nevzat Gözüaydın, Hamza Zülfikar, Belgin Tezcan Aksu, Seyfullah Türkmen, Yaşar Yılmaz, Cilt II, 9. Baskı, Sözlük Bilim ve Uygulama Kolu Yayınları Türkçe Sözlükler Dizisi: 1, Türk Dil Kurumu Yayınları: 549, Ankara.

Türk Dil Kurumu Türkçe Sözlük, (2005), Hazırlayanlar: Şükrü Halûk Akalın, Recep Toparlı, Nevzat Gözüaydın, Hamza Zülfikar, Mustafa Argunşah, Nurettin Demir, Belgin Tezcan Aksu, Beyza Gültekin, 10. Baskı, Türk Dil Kurumu Yayınları: 549, Ankara.

TÜRKİYE BÜYÜK MİLLET MECLİSİ, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)*, Yasama Dönemi: 24, Yasama Yılı: 3, Sıra Sayısı: 380, https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, ET. 2 Mart 2020.

Uçar Hüdaverdi (2014), *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları*, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı Yüksek Lisans Tezi, Ankara, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

ULAKNET, "Ulaknet Kullanım Politikası", https://ulakbim.tubitak.gov.tr/sites/images/Ulakbim/ukp-v2011.pdf, ET. 27 Ekim 2019.

Uludoğan Mustafa (Ocak 2002), *Eğitimde Bilgisayar Okur Yazarlığı Bilgisayara Giriş Ders Kitabı,* Atlas Yayın Dağıtım, İstanbul.

Ulutaş Güzin (2018), "Siber Güvenlik", *Siber Güvenlik ve Savunma : Farkındalık ve Caydırıcılık*, Editör: Şeref Sağıroğlu, Mustafa Alkan, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Ankara, Grafiker Yayınları, ss. 87- 101.

UNITED NATIONS, "Birleşmiş Milletler Dijital Kütüphanesi", https://digitallibrary.un.org/, ET. 28 Şubat 2020.

UNODC, https://www.unodc.org/, ET. 28 Şubat 2020.

UNODC, https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html, ET. 28 Şubat 2020.

UNODC, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html, ET. 1 Mart 2020.

UNODC, INTERNATIONAL TELECOMMUNICATION UNION *"Cybercrime : The Global Challenge"*, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf, ET. 28 Şubat 2020.

Ünal Ahmet (2014), *Bilişim Suç Türlerinden Biri Olan Dağıtık Servis Dışı Bırakma (DDoS) Saldırılarının Önlenmesindeki Hukuki ve Teknik Zorluklar*, İstanbul Bilgi

Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

Ünal Ahmet Naci (2015), *Siber Güvenlik ve Elektronik Bileşenleri*, Nobel Akademik Yayıncılık, Ankara.

Ûzcan Sinan, "Güvenilir Sanal Özel İntranet", ss. 59-60, http://www.emo.org.tr/ekler/071cfa81605a94a_ek.pdf, ET. 27 Ekim 2019.

www.kazanci.com›kho2/ibb/giris.html, ET. 15 Temmuz 2020.

Yaşar Osman, Gökcan Hasan Tahsin, Artuç Mustafa, (2014), *Yorumlu – Uygulamalı Türk Ceza Kanunu*, 5. Cilt, Tamamen Gözden Geçirilmiş 2. Baskı, Adalet Yayınevi, Ankara.

Yaycı Esra (2007), *Bilişim Suçları*, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Ceza ve Ceza Usulü Hukuku Bilim Dalı, Master Tezi, Ankara, https://tez.yok.gov.tr/UlusalTezMerkezi/, ET. 14 Temmuz 2020.

Yazıcı Pınar (2011), "Ulusal Mevzuat ve Yargıtay İçtihatları Işığında Türk Ceza Kanunu'ndaki "Bilişim Alanında Suçlar"", Prof. Dr. Belgin Erdoğmuş'a Armağan (Derleyen: M. Murat İnceoğlu), *Der Yayınları*, İstanbul, ss. 909-928.

Yazıcıoğlu Recep Yılmaz (1997), *Bilgisayar Suçları : Krimonolojik, Sosyolojik ve Hukuki Boyutları İle*, Alfa Yayınları, İstanbul.

Yazıcıoğlu Recep Yılmaz (1999), "Şifreli Yayınların Bilişim Suçları Karşısındaki Konumu", *Yargıtay Dergisi*, Cilt: 25, Sayı: 1-2, Ocak-Nisan 1999.

Yazıcıoğlu Yılmaz (2002), *"Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı"*, Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001, İzmir: Dokuz Eylül Üniversitesi Yayını, ss. 451-470.

Yazıcıoğlu Yılmaz (2008), "Hackerler ve Bilişim Sistemine Girme Suçu (TCK. MD.243)", Ord. Prof. Dr. Sulhi Dönmezer Armağanı, Cilt II, *Atatürk Kültür, Dil ve Tarih Yüksek Kurumu Atatürk Araştırma Merkezi Türk Ceza Hukuku Derneği*, Ankara, ss. 1239-1261.

Yeğin Alper E. (2006) "IPv6-İnternet Protokolü Sürüm 6", *Türkiye Bilişim Ansiklopedisi*, Başeditörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen, 1.Basım, Türkiye Bilişim Vakfı, Papatya Yayıncılık, İstanbul, ss. 499-503.

Yenidünya Caner, Değirmenci Olgun (2003), *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, Legal Yayıncılık, İstanbul.

Yetim Servet (2014), "Bilişim Suçları ve Etkin Mücadele Yöntemleri", *Terazi Aylık Hukuk Dergisi*, Cilt: 9, Sayı: 95, Temmuz 2014, ss. 80- 86.

Yıldırım Esen, "C++ Programlama, MKÜ - Bilgisayar Mühendisliği Algoritmalar ve Programlama Ders Notları", http://hpss.endustri.cu.edu.tr/ders/ENS255/383_dosya_1341385774.pdf, ET. 12 Ekim 2019.

Yılmaz Sacit (2011), "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", *Türkiye Barolar Birliği Dergisi,* Sayı: 92, Yıl: 23, Ocak-Şubat 2011, ss. 62-100.

Yılmaz Seda ve Sağıroğlu Şeref (2013), "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", *ISC Turkey 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*, Bildiriler El Kitabı, 20-21, Ankara, Eylül 2013, s. 158-166, https://vdocuments.mx/siber-guevenlik-risk-analizi-tehdit-ve-hazirlik-seviyeleri.html, ET. 11 Şubat 2020.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Soyisim, İsim : GÜN, Nagihan

Uyruğu : T.C.

Doğum Tarihi ve Yeri : 27.09.1989 / Zonguldak

Medeni Hali : Bekar

E-posta : nagihan.gun@hotmail.com

EĞİTİM

DERECE	KURUM	MEZUNİYET YILI
Lise	Zonguldak Atatürk Anadolu Lisesi	2007
Lisans	Kocaeli Üniversitesi Hukuk Fakültesi	2011

İŞ DENEYİMİ

YIL	YER	POZİSYON
2011-2012	Zonguldak Barosu	Stajyer Avukat
2012-2018	Çevre ve Şehircilik Bakanlığı	Avukat
2018- Halen	Bilgi Teknolojileri ve İletişim Kurumu	Bilişim Uzman Yardımcısı