BİLİŞİM SİSTEMİNE GİRME SUÇU

ALP ÖZTEKİN

HAZİRAN 2022

ÇANKAYA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

KAMU HUKUKU YÜKSEK LİSANS TEZİ

BİLİŞİM SİSTEMİNE GİRME SUÇU

ALP ÖZTEKİN

HAZİRAN 2022

ÖZ

BİLİŞİM SİSTEMİNE GİRME SUÇU

ÖZTEKİN, Alp
Kamu Hukuku Yüksek Lisans Tezi

Danışman: Dr. Burcu ERTEM
Haziran 2022, 264 sayfa

TCK md. 243'te iki ayrı suç birlikte düzenlenmiştir. Maddenin ilk üç fıkrasında yetkisiz erişim suçu, dördüncü fıkrasında ise araya girme suçu düzenlenmiş olup her iki suç da 765 s. mülga TCK'da tam karşılığı bulunmayan, esas olarak 5237 s. TCK'da ilk olarak yürürlüğe konulmuş suçlardır. Bu düzenlemeler, Türkiye'nin de tarafı olduğu ve yürürlükte bulunan Avrupa Siber Suçlar Sözleşmesi'nin ikinci ve üçüncü maddelerindeki düzenlemeler ile tamamen paraleldir. Yetkisiz erişim suçu ile korunması amaçlanan hukuksal değer, bilişim sistemleri üzerindeki yetkili olma durumundan kaynaklı haklar ve buna bağlı dokunulmazlıktır. Araya girme suçu ile korunması amaçlanan hukuksal değer ise veri trafiğinin gizliliğine dair haktır. Fail ile mağduru herkes olabilen ve neticesi harekete bitişik durumdaki bu suçlarda; yetkisiz erişim suçu yönünden hedef sisteme erişimin gerçekleşmiş olması, araya girme suçu yönünden de veri nakillerinin teknik araçla araya girilerek izlenmesi neticesinde illiyet bağı da kurulabiliyor ise objektif tipiklik oluşacaktır. Sistemdeki verilerin yahut nakil halindeki verilerin içerdiği bilgilerin öğrenilmesi ise suçun objektif tipikliğinin oluşumu açısından gerekmemektedir. Maddede düzenlenen her iki suç yönünden de teşebbüs mümkündür. Yetkisiz erişim suçunun konusu bilişim sistemi olup, araya girme suçunun konusu ise nakil halindeki verilerdir.

Yetkisiz erişim suçunun konusu bedeli karşılığı yararlandırılan bilişim sistemleri ise bu durumda maddenin ikinci fıkrasında yer alan hafifletici sebep düzenlemesi tatbik edilecektir. Maddenin üçüncü fıkrasında ise kast + taksir kombinasyonu teşkil eden gerçek bir neticesi sebebiyle ağırlaşmış suç düzenlemesine gidilmiş ve yetkisiz erişim suçunun, verilerin yok olması veya değişmesi neticesine bağlı neticesi sebebiyle ağırlaşmış hali oluşturulmuştur. Her iki suç yönünden de sübjektif tipikliğin oluşumu için kast ve hukuka aykırılık bilinci gerekli olup, failde belirli bir saikin mevcudiyeti aranmamaktadır. Yetkisiz erişim suçu ile TCK'da yer alan bütün yazılı hukuka uygunluk sebepleri bağdaşmakta ise de meşru savunma yönünden kesin bir teorik çıkarım yapılamamaktadır. Araya girme suçu yönünden ise meşru savunma dışındaki hukuka uygunluk sebeplerinin gündeme gelmesi mümkündür. Suçların kınanabilirlik unsuru yönünden ise tartışılabilecek herhangi bir özel durum bulunmamaktadır. Hacking olayları sonucunda meydana gelebilen bu suçlarda zincirleme suç hükümlerinin uygulanması mümkün olup, suçların işlenmesi sırasında farklı suçların meydana gelme olasılığı da kuvvetli olduğundan, bu suçlara yönelik içtima noktasında titiz bir inceleme yapılması gerekmektedir. TCK md. 243'te düzenlenen yetkisiz erişim ve araya girme suçları işlendiği sırada sair suçlara da sebep olunması durumunda fikri içtima durumu değerlendirilmeli, fikri içtimanın şartları oluşmuyor ise daima gerçek içtima uygulanmalıdır. Zira bu suçların bileşik suç niteliğinde değerlendirilebileceği bir düzenleme maddi ceza hukukumuzda bulunmamaktadır. Bu suçların sübut bulması halinde tüzel kişiler hakkında da gerçek kişiler ile birlikte güvenlik tedbirlerine hükmedilmesi mümkün olup, bu noktada eşya müsaderesi ve bilişim sistemlerinin müsadere uygulamalarına konu edilmesi olanak dahilindedir.

Anahtar Kelimeler: Yetkisiz erişim, Araya girme, Sistem, Saldırı, Trafik, Hack.

ABSTRACT

CRIME OF TO ENTER TO IT SYSTEM

ÖZTEKİN, ALP

M.A. in Public Law

Supervisor: Dr. Burcu ERTEM

June 2022, 264 pages

Two separate crimes are regulated together in article 243 of Turkish Criminal Code(*TCK*). The crime of unauthorized access is regulated in the first three paragraphs of the article, the crime of interception is regulated in the fourth paragraph. Both crimes are does not have an exact equivalentrepeal in repealed Code no. 765 and those crimes were put into effect for the first time in the TCK no. 5237. These regulations are in full parallel with the regulations in the second and third articles of the European Cybercrime/Budapest Convention, which Turkey is also a party to and which is in force. The legal value that is aimed to be protected by the crime of interception is the right to privacy of data traffic. All the written reasons for compliance with the law are compatible with the unauthorized access crime. However, no definite theoretical inference can be made in terms of legitimate defense. It is possible to apply the reasons of compliance with the law other than self-defence in terms of the interception crime. In these crimes, the perpetrator and the victim of which can be anyone and the results of crimes are adjacent to the action. If a causal link can be established; as a result of access to the target system in terms of unauthorized access crime and monitoring of data transmissions by interfering with technical means in terms of the crime of interception, objective typicality will occur. Learning the data in the system or the information contained in the data in transit is not necessary for the formation of the objective typicality of the crime.

Attempt to a crime is possible in terms of both offenses regulated in the article. The subject of the crime of unauthorized access is the IT system, and the subject of the crime of interception is the data in telecommunication traffic. If the subject of the crime of unauthorized access is the IT systems made available for the price, in this case, the mitigating circumstance regulation in the second paragraph of the article will be applied. In the third paragraph of the article, a real crime aggravated by the result has been regulated which is a combination of caste + negligence and depending to the result of the destruction or change of data, aggravated form of unauthorized access crime has been created. Consciousness of intent and illegality is necessary for the formation of subjective typicality in terms of both crimes, and the presence of a specific motive is not sought in the perpetrator. The legal value that is aimed to be protected by the crime of unauthorized access is the rights arising from the authority on the information systems and the immunity related to it. There is no special situation that can be discussed in terms of the reprehensibility element of the crimes. It is possible to apply chain crime provisions in these crimes that may occur as a result of hacking events, since the possibility of different crimes to occur during the commission of crimes is strong, a meticulous examination should be made at the point of collection for crimes. The intellectual collection situation should be evaluated when other crimes are also caused while the crimes of unauthorized access and interception regulated in article 243 of TCK are committed. If the conditions of the intellectual collection are not met, the real collection should always be applied. Because there is no regulation in our substantive criminal law where these crimes can be considered as compound crimes. If these crimes are proven, it is possible to apply security measures to legal persons as natural persons. At this point, it is possible to confiscating of goods and IT systems.

Keywords: Unauthorized acccess, Interception, System, Attack, Traffic, Hack.

TEŞEKKÜR

Bu çalışma sırasında; değerli vaktini ayırarak tez çalışması ile ilgili her türlü bilgi, yardım ve katkıyı benden esirgemeyen, belirli kalıplaşmış olguları dikte etmek yerine gerçek bir hukukçu olarak bilimsel düşünce ekseninde kendimi geliştirebilmeme olanak tanıyan, mesleğine olan sevgisi ve takdire şayan vaziyetteki icra şeklini gelecekteki meslek hayatım için örnek aldığım tez danışmanım sayın Dr. Burcu Ertem'e en içten saygılarımla teşekkür ederim.

İÇİNDEKİLER

KISALTMALAR LİSTESİ

agb.	: Adı Geçen Belge
age.	: Adı Geçen Eser
ASS	: Avrupa Siber Suçlar Sözleşmesi
AYM	: Anayasa Mahkemesi
Bkz.	: Bakınız
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CAN	: Campus Area Network (Kampüs Alan Ağı)
CCDCOE	: Cooperative Cyber Defence Centre of Excellence (Müşterek Siber Savunma Mükemmeliyet Merkezi)
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
DHCP	: Dynamic Host Configuration Protocol (Dinamik Host Yapılandırma Protokolü)
E.	: Esas Numarası
ET	: Erişim Tarihi
FBI	: Federal Bureau of Investigation (Federal Soruşturma Bürosu)
HD.	: Hukuk Dairesi
INTERPOL	: The International Criminal Police Organization (Uluslararası Kriminal Polis Teşkilatı)
IoT	: Internet Of Things (Nesnelerin İnterneti)
IP	: Internet Protocol (İnternet Protokolü)
İSS	: İnternet Servis Sağlayıcı
K.	: Karar Numarası
LAN	: Local Area Network (Yerel Alan Ağı)
MAC	: Media Access Control (Medya/Ortam Erişim Protokolü)

MAN	: Metropolitan Area Network (Büyükşehir Alan Ağı)
MASAK	: Mali Suçlar Araştırma Kurulu Başkanlığı
md.	: Madde
MITM	: Man In The Middle (Ortadaki Adam)
M2M	: Machine To Machine (Makineden Makineye İletişim)
NAT	: Network Address Translation (Ağ Adresi Çevirisi)
Örn.	: Örneğin
SQL	: Structured Query Language (Yapılandırılmış Sorgu Dili)
s.	: Sayfa
SİHA	: Silahlı İnsansız Hava Aracı
TCK	: Türk Ceza Kanunu
TMK	: Türk Medeni Kanunu
TMK	: Terörle Mücadele Kanunu
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
XSS	: Cross Site Scripting (Siteler Arası Betik Çalıştırma)
WAF	: Web Application Firewall (Web Uygulama Güvenlik Duvarı)
vb.	: Ve Benzeri
WAN	: Wide Area Network (Geniş Alan Ağı)

GİRİŞ

Tez konusu olan TCK md. 243, Avrupa Siber Suçlar Sözleşmesi'nde iki ayrı maddede düzenlenen iki farklı suçu bünyesinde barındırmaktadır. Bu suçlar maddenin ilk üç fıkrasında düzenlenen ‘’yetkisiz erişim‘’ suçu ve dördüncü fıkrasında düzenlenen ‘’araya girme‘’ suçudur. Her ne kadar madde başlığı ‘’bilişim sistemine girme‘’ şeklinde oluşturulmuş ise de ilk üç fıkrada düzenlenen suçun uluslararası hukuki metinler ve sair ülke mevzuatları ile uygulamadaki isimlendirilmesi, ‘’yasa dışı-gayri meşru-yetkisiz-izinsiz erişim‘’ şeklindedir. Avrupa Siber Suçlar Sözleşmesi'nin ikinci maddesinde ‘’illegal access‘’ şeklinde bir isimlendirme yapılmış ise de kanaatimizce bunun Türkçe çevirisi olan ‘’hukuka aykırı erişim‘’, yanlış bir isimlendirme olacaktır. Zira hukuka uygun erişimin bir suç olması ve hatta hiçbir fiilin hukuka uygun halinin bir suç olması düşünülemeyeceğinden, bu isimlendirme suçun temel özelliklerini aktarmada yetersiz kalmaktadır. Ayrıca hukuka aykırı erişimi hukuka uygun kılmak şeklinde mantığa aykırı bir yorum yapılamayacağı, hukuka uygunluk sebebi bulunuyorsa durumun zaten hukuka uygun olacağı gereğince, böyle bir isimlendirmede hukuka uygunluk sebepleri de mantıklı biçimde açıklanamamaktadır. Öyleyse TCK md. 243'ün ilk üç fıkrasında düzenlenen suçun, (*18. Başlık*)18 Sayılı Federal ABD Ceza Kanunu'nun 1030. maddesi ve eyalet ceza kanunlarında düzenlendiği şekliyle ‘’unauthorized access‘’ yani ‘’yetkisiz erişim‘’ şeklinde isimlendirilmesi, suça konu fiilin de bu şekilde tanımlanması doğru olacaktır. Bu sebeple işbu tez içerisinde suç bu şekilde isimlendirilmiştir. Avrupa Siber Suçlar Sözleşmesi'nde araya girme suçu isimlendirilirken de başına ‘’illegal‘’ nitelemesi konulmuştur. Belirtildiği üzere bir suç normunun isimlendirilmesinde ‘’hukuka aykırı‘’ şeklinde bir niteleme yapılmaması gerektiğinden, bu suç yönünden de işbu tez kapsamında yalnızca ‘’araya girme suçu‘’ şeklinde bir isimlendirme yapılmıştır.

Araya girme suçu yönünden ‘’yetkisiz‘’ şeklinde bir nitelendirmenin tarafımızca isimlendirme noktasında yapılmıyor oluşunun temel gerekçesi ise ‘’erişim‘’ fiilinin genel manası yetkili olma durumunu içerdiğinden ve yetkisiz erişimler istisnai iken, araya girme durumlarının bizatihi ekseriyetle yetkisizlik içeriyor olmasıdır. Nasıl ki TCK md. 132’nin başlığı ‘’yetkisiz olarak haberleşmenin gizliliğini ihlal‘’ değil ise ve haberleşmenin gizliliğinin ihlal edilmesi ekseriyetle zaten yetkisizlik yaratıyor ise araya girme suçu yönünden de benzer bir vaziyetin mevcudiyeti kabul edilmelidir.

Türk hukuk doktrininde spesifik kaynaklar haricinde; yetkisiz erişim suçunun önemi yeterince kavranamamış olup, araya girme suçu ise nadiren üzerinde etraflıca durulan bir suç türü durumundadır. İçtihatlar noktasında da durum benzerdir. Bunun sebebi sanıyoruz ki yetkisiz erişimin sair bilişim suçlarının işlenebilmesi için yapılan zaruri faaliyetler gibi algılanması, araya girme suçunun ise pratikte ne şekilde gerçekleşebileceğinin çoğu zaman kavranamamasıdır. Halbuki bu suçlar bilişim suçlarının özüdür. Bu suçların çoğu hacking faaliyetinde tek başına oluşma ihtimali oldukça kuvvetli olduğu gibi diğer suçlar ile birlikte işlendikleri zaman içtima yönünden doğru bir yorum yapılabilmesi için bu suçların sınırlarının doğru bilinmesi gerekir. Tez konusu suçların özünde ne ifade ettiğinin ve bu suçların tipiklik unsurunun doğru anlaşılabilmesi, bunun da ötesinde suç normlarına dair faydalı eleştirilerde bulunulabilmesi için ise suçların konusu olan bilişim sistemlerinin ve suçların işlenme şekillerinin iyi bilinmesi gerekmektedir. Bu sebeple tez içerisinde açıklamalar bu konulara ehemmiyet verilerek kaleme alınmış, suçun unsurları aktarılırken mümkün mertebe hacking olayları ile ilişkilendirilerek konular anlatılmıştır.

BÖLÜM I

YETKİSİZ ERİŞİM VE ARAYA GİRME SUÇLARINA DAİR GENEL AÇIKLAMALAR

1.1. YETKİSİZ ERİŞİM VE ARAYA GİRME SUÇLARININ TÜRK HUKUKUNDAKİ TARİHSEL GELİŞİM SÜRECİ

765 s. Türk Ceza Kanunu'nun[1] 525/a maddesinde, bugün yürürlükte bulunan ve bu tezin de konusunu oluşturan suçlara kısmen benzer bir ceza normu bulunuyordu. Bilişim sistemlerinin toplumsal hayatta yerini almasıyla birlikte 1991 yılında 765 s. mülga kanuna eklenen ilgili 525/a maddesi şu şekildedir:

> ''*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.*''

Mülga normun yürürlükteki 5237 s. Türk Ceza Kanunu[2] md. 243'ün ilk üç fıkrasında düzenlenen yetkisiz erişim(*bilişim sistemine girme*) ve maddenin dördüncü fıkrasında düzenlenen araya girme suçları ile bağlantılı yönü

> ''*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.*''

şeklindeki kısımdır. Mülga normun bu kısmında bilişim verilerinin ele geçirilmesi fiili normun tipikliği içerisinde düzenlenmiş olup, verilerin ele geçirilmesi

[1] Yayımlandığı Resmi Gazete: Tarih: 13/3/1926 Sayı: 320
[2] Yayımlandığı Rersmi Gazete: Tarih: 12/10/2004 Sayı: 25611

de sisteme erişilerek veya sisteme erişmeden salt araya girilerek gerçekleştirilebileceğinden,[3] 243. maddedeki her iki suçun da mülga normun tipikliği içerisinde zımnen düzenlendiği sonucuna varılabilir.

Mülga norm ile 5237 s. TCK md. 243 arasındaki temel fark ise aşağıda detaylı olarak aktarıldığı üzere, mülga normun aksine yetkisiz erişim ve araya girme suçlarında verilerin ele geçirilmesinin suçun tipikliğine konu bir unsur olarak düzenlenmemiş olmasıdır. Bu ele geçirme durumu; özel olarak kişisel veriler, fikri ve sınai haklar yahut mal varlığına dair hakları koruyan maddi ceza normlarının tipikliği içerisine girer. Öyleyse temel hali TCK md. 243/1'de düzenlenen yetkisiz erişim suçunun verileri ele geçirme ve dolayısıyla da mülga norm ile bir bağı kalmadığı anlaşılmaktadır. Dördüncü fıkrada düzenlenen araya girme suçu yönünden de benzer bir yorumun yapılması mümkündür.

Budapeşte/Avrupa Siber Suçlar Sözleşmesi(*ASS*) 2001 yılında ilk imzacıları tarafından kabul edilmiş olup, bilişim suçları yönünden çerçeve uluslararası normlar bu sözleşme ile oluşturulmuştur. Genel esasları doksanlı yıllarda oluşmaya başlamış olan ASS'nin oluşum süreçlerinden önce de bilişim sistemleri toplumsal kullanımda belirli bir yaygınlığa ulaştığından, Türkiye'nin de 765 s. Kanun'daki düzenlemeler ile içerisine dahil olduğu çeşitli hukuk sistemlerinde, ASS'den evvel de bilişim suçlarına dair cezai normlar bulunuyordu. İlk imzacı ülkelerde sözleşmenin yürürlüğe girmesinin akabinde sair pek çok hukuk sistemi, sözleşme hükümleri kendisi açısından bağlayıcı olmasa da bilişim suçlarına dair düzenlemeleri sözleşmeye göre uyarlamıştır. Türk hukuku yönünden de bilişim suçlarının gelişimi bu şekilde olmuştur. 5237 s. TCK yürürlüğe girdiğinde pek çok suç gibi bilişim suçları da revize edilmiştir ve ilgili tarihte ülkemiz sözleşmenin imzacısı olmasa da normlar incelendiğinde bu revizenin büyük oranda ASS'ye entegre biçimde yapıldığı anlaşılmaktadır.[4]

5237 s. TCK'nın 243. maddesinde, evvela madde başlığında zikredilen ve bizim ''*yetkisiz erişim suçu*'' şeklinde isimlendirdiğimiz *bilişim sistemine girme suçu* birinci, ikinci ve üçüncü fıkralarda düzenlenmiştir. Oluşumu için verilerin gönderici ve alıcı pozisyonundaki sistemlere erişilmeden işlenmiş olması gereken *araya girme suçu* ise maddenin dördüncü fıkrasında düzenlenmiştir.

[3] Bir bilişim sisteminde depolanmış verilerin başka bir sisteme iletimi halinde, bu veriler pekala iletişim kanalı üzerinden yakalanarak ele geçirilebilir. Mülga kanunun ilgili maddesinden de salt sistemler içerisindeki depolanmış verilerin kastedildiğine yönelik bir anlam çıkarılamamaktadır.
[4] ASS 2010 yılında imzalanmış, 2014 yılında da ülkemizde yürürlüğe girmiştir.

Maddenin ‘’*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.*‘’ şeklindeki birinci fıkrası, yetkisiz erişim suçunun temel halidir. Eskiden normun ‘’*giren veya orada kalmaya devam eden*‘’ kısmındaki ‘veya’ bağlacı, ‘ve’ şeklinde düzenlenmişti. Ancak ‘’kalmaya devam etme‘’ yönüyle suçun neticesinin oluşumu tartışmalı olduğundan, bu bağlaç doktrinde genel olarak eleştirilen bir konuydu.[5] 24.03.2016 tarihinde, ilgili 243. maddede değişiklik yapan 6698 s. Kişisel Verilerin Korunması Kanunu’nun[6] 30. maddesinin yürürlüğe girmesi ile 243. maddenin birinci fıkrasındaki bağlaç ‘veya’ şeklinde değiştirilmiştir. Yine maddenin ilk halinde bulunmayan dördüncü fıkradaki araya girme suçu da maddeye 6698 s. Kanun’un 30. maddesinin yürürlüğe girmesi ile eklenmiştir.

Suçun nitelikli hallerinden cezayı hafifletici sebebi düzenleyen kısım, maddenin ‘’*Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler* hakkında *işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.*‘’ şeklindeki ikinci fıkrasıdır. Yetkisiz erişim suçunun neticesi sebebiyle ağırlaşmış hali[7] ise maddenin üçüncü fıkrasında ve ‘’*Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.*‘’ şeklinde düzenlenmiştir.

[5] Ali KARAGÜLMEZ (2014), *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Beşinci Basım, Seçkin, Ankara, s. 229.
[6] Yayımlandığı Resmî Gazete: Tarih: 7/4/2016 Sayı: 29677
[7] Üçüncü fıkradaki durum, gerçek neticesi sebebiyle ağırlaşmış suçu, yani kast+taksir kombinasyonunu teşkil etmektedir.

Ayrı bir suç olan[8] araya girme suçu ise maddenin dördüncü 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.*‘’

şeklinde düzenlenmiş olup, hukukumuzda araya girme suçu yönünden bir hafifletici sebep öngörülmemiştir.

3713 s. Terörle Mücadele Kanunu'nun[9] dört ve beşinci maddelerinde her iki suç yönünden de bir ağırlaştırıcı sebep düzenlemesi bulunmaktadır. 3713 s. Kanun'un 4. maddesinde, TCK md. 243'teki suçların 3713 s. Kanun'un birinci maddesinde belirtilen amaçlar doğrultusunda, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde terör suçu sayılacağı düzenlenmiş ve aynı Kanun'un beşinci maddesinde cezada artırım öngörülmüştür.[10]

1.2. ULUSLARARASI HUKUKİ METİNLERDE YETKİSİZ ERİŞİM VE ARAYA GİRME SUÇLARINA DAİR DÜZENLEMELER

Etki alanı ve bağlayıcılık yoğunluğu farklı olmakla birlikte, bugün için siber suçlar/bilişim suçları alanında çerçeve düzenlemeler getiren pek çok uluslararası metin bulunmaktadır. Bunlardan görece önemli olanları Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Anlaşması, Batı Afrika Devletleri Ekonomik Topluluğu Siber Suçla Mücadele Direktifi Taslağı, Arap Devletleri Ligi Bilgi

---

[8] Doktrindeki hakim görüş de dördüncü fıkrada düzenlenen araya girme suçunun yetkisiz erişim suçundan bağımsız bir suç olduğudur. Bu konuda bkz. Köksal BAYRAKTAR, Zeynel T. KANGAL, Vesile Sonay EVİK, Ali Kemal YILDIZ, Eylem Aksoy RETORNAZ, Gülşah Bostancı BOZBAYINDIR, Pınar Memiş KARTAL, Ali Hakan EVİK, Asuman Aytekin İNCEOĞLU ve Fulya EROĞLU (2021), *Özel Ceza Hukuku C. VIII Ekonomi, Sanayi ve Ticarete İlişkin Suçlar-Bilişim Alanında Suçlar*, Onikilevha, İstanbul, s. 231, 232; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK (2021), *Teorik ve Pratik Ceza Özel Hukuku*, Ondokuzuncu Basım, Seçkin, Ankara, s. 1161; Mahmut KOCA ve İlhan ÜZÜLMEZ (2020), *Türk Ceza Hukuku Özel Hükümler*, Yedinci Basım, Adalet, Ankara, s. 895; Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE (2021a), *Türk Ceza Hukuku Özel Hükümler*, Onaltıncı Basım, Seçkin, Ankara, s. 962; Berrin AKBULUT (2017), *Bilişim Alanında Suçlar*, İkinci Basım, Adalet, Ankara, s. 112. / Doktrinde araya girme suçunun yetkisiz erişim suçu ile birlikte düzenlenmesinin hatalı olduğu ve bizim de katıldığımız üzere ayrı bir maddede düzenlenmesi gerektiği yönünde görüşler için bkz. Murat Volkan DÜLGER (2022), *Bilişim Suçları ve İnternet İletişim Hukuku*, Dokuzuncu Basım, Seçkin, Ankara, s. 245; Nagihan GÜN (2020), *Türk Ceza Hukukunda Bilişim Suçları,* Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara, s. 205.

[9] Yayımlandığı Resmî Gazete: Tarih: 12/4/1991 Sayı: 20843 Mükerrer

[10] Beşinci maddenin ilgili kısmı şu şekildedir: ‘’*3 ve 4 üncü maddelerde yazılı suçları işleyenler hakkında ilgili kanunlara göre tayin edilecek hapis cezaları veya adlî para cezaları yarı oranında artırılarak hükmolunur. Bu suretle tayin olunacak cezalarda, gerek o fiil için, gerek her nevi ceza için muayyen olan cezanın yukarı sınırı aşılabilir. Ancak, müebbet hapis cezası yerine, ağırlaştırılmış müebbet hapis cezasına hükmolunur. Suçun, örgütün faaliyeti çerçevesinde işlenmiş olması dolayısıyla ilgili maddesinde cezasının artırılması öngörülmüşse; sadece bu madde hükmüne göre cezada artırım yapılır. Ancak, yapılacak artırım, cezanın üçte ikisinden az olamaz.*‘’

Teknolojilerine Karşı Saldırılarla Mücadele Anlaşması ve en önemlileri ise ülkemizde de yürürlükte bulunan Avrupa Siber Suçlar Sözleşmesi'dir.[11] Bunlar arasından iç hukukumuz yönünden bağlayıcılığı bulunan tek metin ASS olduğundan, işbu başlıkta sadece TCK paralelinde düzenlemeler içeren ASS'nin ilgili hükümleri aktarılmıştır.

Avrupa Siber Suçlar Sözleşmesi(*Budapeşte Sözleşmesi-ETS No. 185*), hazırlıkları yıllar öncesinden başlamış ve 2001 yılında imzaya açılmıştır.[12] Bu sözleşme dar manadaki bilişim suçlarını maddi ceza hukuku yönüyle düzenlemekte ve bu suçlarla mücadeleye yönelik usul hükümleri ile cezalandırmaya dair normları da içermektedir. ASS 2014 yılında ülkemizde de kanun ile uygun bulunarak yürürlüğe girmiştir.[13] Sözleşmenin iki adet ek protokolü mevcut olup, bu ek protokollerden ilki ırkçılık ve yabancı düşmanlığı, ikincisi ise elektronik deliller ile ilgilidir.[14] Halihazırda Türkiye de birinci ek protokolün imzacısıdır.[15]

TCK md. 243'te düzenlenen ilk suç olan yetkisiz erişim suçunun ASS'deki tam karşılığı, sözleşmenin ikinci maddesindeki düzenlemedir.[16] Yasadışı erişim başlığını taşıyan düzenleme şu şekildedir:

> ''*Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezai 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 sahtekar niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir.*''

İlgili düzenlemede dikkat çeken ilk husus, normda ''haksız yere'' denilerek haksızlık bilincine yollama yapılmış olmasıdır. İkinci olarak normda, imzacı devletler tarafından iç hukuklarında suçun ancak kasten işlenebileceğine yönelik

---

[11] Bilişim suçları alanında ASS haricindeki uluslararası hukuki metinlere dair detaylı açıklamalar için bkz. Merve ERDEM ve Gürkan ÖZOCAK (2019), ''Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Hukukun Rolü''*, Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C. 68, S. 1, ss. 127-212, s. 160, 161, 162, 163 vd.

[12] Sözleşmenin oluşum sürecine dair detaylı açıklamalar için bkz. Murat Volkan DÜLGER 2022, age. s. 203, 204 vd.

[13] https://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm, (ET: 02.03.2022).

[14]Ek protokoller ve bunlara erişim bağlantısı için bkz. https://www.coe.int/en/web/portal/home?p_p_id=15&p_p_lifecycle=0&p_p_state=pop_up&p_p_mode=view&_15_groupId=99928066&_15_struts_action=/journal/preview_article_content&_15_articleId=99928932&_15_version=1.3), (ET: 02.03.2022).

[15] https://www.coe.int/en/web/cybercrime/-/turkey-signed-the-protocol-on-racism-and-xenophobia, (ET: 02.03.2022).

[16] Aynı yönde bkz. Murat Volkan DÜLGER 2022, age. s. 246; Ali PARLAR ve Muzaffer HATİPOĞLU (2010), *Türk Ceza Kanunu Yorumu Cilt 4*, Üçüncü Basım, Seçkin, Ankara, s. 3741.

düzenlemelerin yapılması gerektiği ortaya konulmuştur. Üçüncü önemli husus ise suçun objektif tipikliğinin oluşmasına yönelik, verilerin elde edilmesi ya da sisteme dair siber güvenlik önlemlerinin aşılmasının ve suça konu sistemin hafif ya da yüksek seviye önlemler ile korunuyor olmasının şart koşulup koşulmayacağının, normu kendi iç hukuk sistemlerine adapte edecek olan imzacı ülkelerin keyfiyetine bırakılmış olmasıdır.[17]

TCK md. 243'te düzenlenen ikinci suç olan araya girme suçunun ASS'deki tam karşılığı ise sözleşmenin üçüncü maddesindeki düzenlemedir. Yasadışı araya girme başlığını taşıyan ilgili norm şudur:

> ''*Taraflardan her biri, bilgisayar verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dahil 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 cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, sözkonusu suçun sahtekarlığa yönelik veya başka bir bilgisayar sistemine bağlı bir bilgisayasar sistemiyle ilişkili olarak işlenmiş olmasını şart koşabilir.*''

Bu düzenlemede de haksızlık bilinci ve kastın gerekliliği ortaya konulmuş, sübjektif tipikliğe dair sahtekarlık saiki şartına ve/veya objektif tipikliğe dair olarak suçun ''*başka bir bilgisayar sistemine bağlı bir bilgisayasar sistemiyle ilişkili olarak işlenmiş olması*'' şartına dair getirilebilecek düzenlemeler ise imzacı ülkelerin keyfiyetine bırakılmıştır.

ASS'nin 13. maddesinde bu suçlara yönelik yaptırım ve tedbirlere dair şu şekilde bir düzenleme bulunmaktadır:

> ''*Taraflardan her biri, 2 ila 11. maddelerde tanımlanan cezai suçların, hürriyetten yoksun bırakmayı da kapsayan etkili, orantılı ve caydırıcı yaptırımlarla cezalandırılabilmesini sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. 2) Taraflardan her biri, madde 12 uyarınca sorumlu tutulan tüzel kişilerin maddi yaptırımlar da dahil olmak üzere etkili orantılı ve caydırıcı cezai veya cezai olmayan yaptırımlara veya tedbirlere tabi olacağını teminat altına alacaktır.*''[18]

[17] TCK'da düzenlenen yetkisiz erişim suçu bakımından suça konu sistemin herhangi bir siber güvenlik önlemi ile korunuyor olması gerekmemektedir.
[18] TCK md. 246'da bu yönde düzenlemeler bulunmaktadır.

1.3. MUKAYESELİ HUKUKTA YETKİSİZ ERİŞİM VE ARAYA GİRME SUÇLARINA BENZER DÜZENLEMELER

1.3.1. Amerika Birleşik Devletleri

Yetkisiz erişim suçu, 18 Sayılı Federal ABD Ceza Kanunu'nun ''*Bilgisayarlarla bağlantılı dolandırıcılık ve ilgili faaliyetler*'' başlıklı 1030. maddesinde düzenlenmiştir. Avrupa Konseyi'nin ABD bilişim suçları mevzuatının ASS ile uyumunu gösteren raporunda da bu bilgi yer almaktadır.[19] İlgili düzenlemede ''*bir bilgisayara yetkisiz olarak erişmek veya yetkili erişimin kapsamını aşmak*'' denilerek, TCK md. 243/1'deki kalmaya devam etmek seçimlik hareketi ile eşlenik bir ikincil seçimlik hareket oluşturulmuştur. 1030. maddenin a üst bendinin 1 ve 3. fıkralarında özel olarak suçun konusu federal hükümet ile ilişkili bilişim sistemleri yahut veriler olup, suçun işlenmesinde de belirli bir saikin varlığı gerekmektedir. 2 ve 4. fıkralar yönünden ise suçun konusu önem arz etmemekle birlikte suça konu neticenin oluşumu için salt hedef sisteme yetkisiz erişim yeterli olmayıp, ikinci fıkrada bilgilere erişim ve dördüncü fıkra yönünden de hem dolandırıcılık amacı(*saik*) hem de menfaat temini neticesi aranmaktadır. Suçun beşinci fıkrasında TCK md. 244'e benzer biçimde sisteme zarar verilmesi objektif tipiklik içerisinde düzenlenmiş, altı ve yedinci fıkralarda ise ticaretin etkilendiği belirli durumlar suç olarak düzenlenmiştir. Öyleyse belirli bilgilere erişim neticesinin aranması dışında ilgili maddenin TCK md. 243/1 ile benzeşen tek düzenlemesi, ikinci fıkradaki düzenlemedir. Suçun b üst bendinde değişik ihtimallere göre çok farklı cezalar öngörülmüş olup, işbu noktada suça dair belirtilebilecek veya örneklendirilebilecek standart bir ceza bulunmamaktadır.

Araya girme suçu, 18 s. Federal ABD Ceza Kanunu'nun ''*Kablolu, sözlü veya elektronik iletişimin ifşası ve araya girilmesi yasaktır*'' başlıklı 2511. maddesinde, ilk fıkranın a bendinde düzenlenmiştir.[20] Her ne kadar Avrupa Konseyi'nin ABD bilişim suçları mevzuatının ASS ile uyumunu gösteren raporunda araya girme suçu ile 18 s. Kanun'un hem 1030 hem de 2511. maddelerinin bağlantılı olduğu zikredilmekte ise de kanaatimizce araya girme suçu yani ASS md. 3 ile bağlantılı tek norm 18 s. Kanun md. 2511'dir. 2511. maddenin ilk fıkrasının diğer bentlerinde ise araya girmeyi

[19] Council of Europe (2008), *United States of America -Cybercrime Legislation-Country Profile*, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b9, (ET: 20.04.2022).

[20] İlgili maddenin sniffing saldırılarını tipikliği içinde barındırdığına yönelik bkz. Sean Philip ORİYANO (2014), *Hacker Techniques, Tools, and Incident Handing*, Jones&Bartlett Learning, USA, s. 281.

sağlayan cihazların kullanımı ve elde edilen bilgilerin ifşası ayrıca suç olarak düzenlenmiş, maddenin kalanında ise genel olarak hukuka uygunluk sebepleri ile suça etki eden haller zikredilmiştir. Araya girme suçunun düzenlendiği ilk fıkranın a bendi şu şekildedir:

> ‘’*(1)Bu bölümde özellikle aksi belirtilmedikçe herhangi bir kişi: (a) Herhangi bir kablolu, sözlü veya elektronik iletişimde kasıtlı olarak araya girer, araya girmeye teşebbüs eder, başka birinin araya girmesini sağlar veya araya girmesine teşebbüs ederse;*‘’.

Kanunun ilgili bölümdeki suçlara dair tanımlamaların yapıldığı 2510. maddesinde araya girme,

> ‘’*Herhangi bir elektronik, mekanik veya sair bir cihazın kullanımı yoluyla herhangi bir kablolu, elektronik veya sözlü iletişim içeriğinin işitsel veya başka şekilde edinilmesi anlamına gelir.*‘’

şeklinde tanımlanmıştır. 2511. maddenin 4. fıkrasının a bendinde ise aynı fıkranın b bendinde belirtilen şifresiz uydu yayınlarına dair suç oluşturmayacak durumlar ve beşinci fıkradaki federal hükümetin davacı olacağı ayrık durumlar haricinde failin para cezasına veya 5 yıla kadar hapis cezasına veya her ikisine birden çarptırılacağı düzenlenmiştir.

1.3.2. Almanya

Avrupa Konseyi’nin Alman bilişim suçları mevzuatının ASS ile uyumunu gösteren raporlarında; Alman Ceza Kanunu(*StGB*) md. 202a’nın yetkisiz erişim yani ASS md. 2, 202b’nin ise araya girme suçu yani ASS md. 3 ile bağlantılı olduğu zikredilmektedir.[21] Kanunun 202a maddesinin başlığı ‘’veri casusluğu‘’ olup, suçu düzenleyen ilk fıkrası,

> ‘’*Her kim kendisi veya başkasının, yetkisiz erişime karşı korunan verilere bu korumayı aşarak yetkisiz erişim sonucu ulaşmasını sağlar ise üç yıla kadar hapis veya para cezasına çarptırılır*.‘’

şeklindedir. Düzenlemenin ikinci fıkrasında ise suça konu verilerin ‘’*elektronik, manyetik veya başka şekilde saklanan ya da iletilen, doğrudan doğruya algılanamayan*‘’ veriler olduğu zikredilmektedir.

[21] Council of Europe (2022), *Germany-Cybercrime Legislation-Domestic Equivalent to the Provisions of the Budapest Convention*, https://rm.coe.int/octocom-legal-profile-germany/1680a5b48b, (ET: 20.04.2022).

ASS md. 2'de ülkelerin yetkisiz erişim suçunun işlenmesini verilerin/bilgilerin elde edilmesi ve/veya sistemin yetkisiz erişimlere karşı korunuyor olması şartına bağlayabileceği düzenlenmiştir. Alman Ceza Kanunu'nun 202a maddesi de bu tercih doğrultusunda oluşturulmuş ve suça konu netice, verilerin ele geçirilmesi olarak düzenlenmiş ve buna bağlı olarak suçun konusu da sistemlerdeki veriler olmuştur. TCK md. 243/1 ile StGB md. 202a'nın bir diğer ayrım noktası da suça konu verilerin yetkisiz erişimlere karşı korunan bir cihazda bulunması ve aynı zamanda suça konu fiilin bu korumanın aşılarak gerçekleştirilmiş olması gereğidir. Kanaatimizce TCK md. 243, ASS ile daha uyumlu ve suçla mücadelede daha etkin bir düzenlemedir. Maddenin lafzı da pratikte tecelli edebilecek haksızlıklara karşı daha açık ve daha kapsayıcıdır.

Avrupa Konseyi tarafından araya girme suçu ile ilişkilendirilen StGB md. 202b ise ''phishing'' başlığını taşımaktadır. Phishing esas olarak bir tabir olup, siber uzay kullanılarak kişisel verilerin ele geçirilmesini konu edinen faaliyetler bütünüdür. Bu konuda işbu tezin hacking yöntemleriyle ilgili açıklamalara bakılarak phishing hakkında detaylı bilgi elde edilebilir. Phishing başlıklı ilgili maddenin içeriği ise araya girme yani veri paketlerinin yakalanması ile ilgilidir. Öyleyse ilgili maddenin başlığının hatalı seçildiği açıktır. 202b maddesinde düzenlenen suçta, 202a maddesindeki verilere yollama yapılarak; bu verileri tarafı olmadıkları kamuya açık olmayan veri iletişimi ya da bir bilgi işlem tesisinden yapılan elektromanyetik yayından teknik yollarla yakalayan kişilerin, suç diğer hükümlere göre daha ağır bir cezaya tabi olmadıkça iki yıla kadar hapis veya adli para cezası ile cezalandırılacakları düzenlenmiştir.

1.3.3. Bangladeş

39 s. Bilişim Teknolojileri Kanunu ve 46 s. Dijital Güvenlik Kanunu'nun yürürlükte olduğu Bangladeş, bilişim suçlarına yönelik müstakil kanunları ve bilişim teknolojilerinin her boyutuyla gündeme gelen haksızlıklara yer verdiği detaylı düzenlemeleriyle bu alanda önemli bir hukuk mevzuatına sahiptir. Ülkede hem 39 hem de 46 s. Kanunlar'da çeşitli bilişim suçları düzenlenmiştir. Yetkisiz erişim suçu esas olarak 46 s. Dijital Güvenlik Kanunu'nun ''*Bilgisayar, dijital cihaz, bilgisayar sistemi ve benzerine hukuka aykırı olarak erişim*'' başlıklı 18. maddesinde düzenlenmiştir. Kanunda her türlü bilişim sistemi ve teknik ekipman yahut ağ yapıları ayrı ayrı detaylı olarak tanımlandığından, maddi ceza normlarında da direkt olarak ''bilişim sistemi''

kavramı geçmemektedir. İlgili 18. maddede de bilgisayar, bilgisayar sistemi veya bilgisayar ağına hukuka aykırı olarak erişmek yahut başkasının erişmesine yardımcı olmak veya sair bir suç işleme maksadıyla bu işlemi gerçekleştirmek suç sayılmıştır. Maddenin ikinci fıkrasında suçun başka bir suç işleme amacıyla işlenmemesi durumunda 6 aya kadar hapis veya 3 aya kadar gün karşılığı adli para cezasına, suçun başka bir suçun işlenmesi amacıyla işlenmesi halinde ise 3 yıla kadar hapis veya 10 yıla kadar gün karşılığı adli para cezasına ya da her ikisine birden hükmedileceği düzenlenmiştir. Üçüncü fıkrada, suça konu bilişim sisteminin siber güvenlik önlemleri ile yetkisiz erişimlere karşı korunuyor olması durumunda 3 yıla kadar hapis ve 10 yıla kadar gün karşılığı adli para cezasına birlikte hükmedileceği düzenlenmiştir. Belirtmek gerekir ki kanunun 34. maddesinde ‘’hacking suçu‘’ düzenlenmiş ve bu suça konu fiillerden biri sisteme yetkisiz eriştikten sonra sisteme zarar vermek olarak zikredilmiştir. Bu suç 18. maddeye göre özel hüküm durumundadır. Hacking suçu işlendiğinde 14 yıla kadar hapis veya 1 yıla kadar adli para cezasına ya da her ikisine birden hükmedilecektir. İlginçtir ki 34. maddenin 2. fıkrasında, hacking suçunda tekerrür halinde müebbet hapse hükmedilebileceği düzenlenmiştir.

Yetkisiz erişim suçunun konusunun ‘’kritik alt yapılar‘’ olması durumunda 46 s. Kanun’un 17. maddesinde ayrık bir suç düzenlenmiştir. Bu suçun cezası ise 18. maddeden daha ağır olarak 7 yıla kadar hapis veya 25 yıla kadar gün karşılığı adli para cezasına ya da her ikisine birden hükmedilmesidir. Failin yetkisiz olarak eriştiği kritik altyapıya dair sistemlere zarar vermesi veya zarar vermeye çalışması durumunda ise 14 yıla kadar hapis veya 1 yıla kadar adli para cezasına ya da her ikisine birden hükmedilecektir. ASS md. 3 ve TCK md. 243/4’te düzenlenen araya girme suçu ile eşlenik spesifik bir düzenlemeye ise Bangladeş ceza hukukunda ulaşılamamaktadır. Sanıyoruz ki bu tür fiiller kişisel veriler ve haberleşmeye dair hakları koruyan maddi ceza normlarının içerisinde değerlendirilmektedir.

BÖLÜM II

YETKİSİZ ERİŞİM VE ARAYA GİRME SUÇLARI İLE İLİŞKİLİ TEMEL KAVRAMLAR

2.1. BİLİŞİM SİSTEMİ

İşbu tez kapsamında hukuki literatüre ve TCK'nın lafzına uygun şekilde, ‘’bilişim sistemi‘’ kavramı kullanılmıştır. Bu sebeple yazılanların iyi kavranabilmesi için okuyucunun, tez kapsamında bilişim sistemi kavramının hangi nitelemeye yönelik kullanıldığına dikkat etmesi gerekmektedir. Bilişim sistemi kavramı, içerisinde hem tekil bilgi-iletişim teknolojisi cihazlarını(*örn. laptop*) hem bu tür cihazların birlikte çalıştığı daha büyük çaplı cihazları(*örn. birkaç m2m cihazdan oluşan robotlar*) ve hem de sistemlerin birbirlerine bağlanarak iletişim kurdukları ağ yapılarını(*örn. yerel alan ağı*) içine alan bir kavramdır. Bu sebeple bilişim sistemi kavramı, kullanım durumuna göre tek bir bilgisayarı da niteleyebilir, yüzlerce bilgisayar ve sair network donanımının bağlı olarak işlediği bir yerel alan ağını da kastedebilir.

Bilişimin Türk Dil Kurumu Sözlüğü'ndeki tanımı şudur:[22]

> ‘’*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.*‘’

Bilişim teknolojisinin Türk Dil Kurumu Sözlüğü'ndeki tanımı ise ‘’*Bilişimde kullanılan bütün araç ve gereçlerin oluşturduğu sistem*‘’ şeklinde yapılmıştır.[23] Sözlükteki bu tanımlar, bilişim sistemi olarak adlandırılan teknolojiler hakkında bir fikir vermekte lakin konuyu yeterince somutlaştıramamaktadır.

[22] Türk Dil Kurumu Sözlük, https://sozluk.gov.tr, (ET: 02.03.2022).
[23] Türk Dil Kurumu Sözlük, https://sozluk.gov.tr, (ET: 02.03.2022).

Doktrinde bilişim; ağ bilişimi, donanım bilişimi ve yazılım bilişimi olarak üç katmana ayrılarak sınıflandırılmaktadır.[24] Bilişim sistemi olarak adlandırılan teknolojilerin ne ifade ettiğinin, kapsamları ile işlevlerinin neler olduğunun kavranabilmesi ve meselenin somutlaştırılabilmesi adına; aşağıda evvela ağ/network, donanım ve yazılım kavramları ile bilişim sistemi kavramının temeli olan veri kavramları açıklanmıştır. Bu alt bileşenlerin açıklanmasından sonra ise bilişim sistemleri salt teknik yönleriyle aktarılmış, bilahare hukuk çerçevesinde bu teknolojilerin sınırlarının ne şekilde çizilmeye çalışıldığı mevzuat, içtihatlar ve doktrin ekseninde açıklanmış, nihayetinde de bilişim sistemlerinin hukuki manada ne ifade etmesi gerektiğine dair şahsi görüş ortaya konulmuştur.

2.1.1. Bilişim Sistemlerine Dair Önemli Alt Kavramlar

2.1.1.1. Donanım ve Yazılım

Bilişim sistemi kavramı; içerisinde tekil bilişim sistemlerini, bunların birlikte çalıştığı daha kapsamlı sistemleri ve birden fazla sistemin bağlı olduğu ağ yapılarını içerisine alan çerçeve bir kavramdır. Aşağıda detaylı olarak açıklandığı üzere bilişim sistemlerini diğer teknolojik aletlerden ayıran temel özellik, veri girdi-çıktısı yapılabilmesi ve otomatik olarak çalışarak, veriler üzerinde çeşitli işlemler gerçekleştirilebilmesini sağlamasıdır. Öyleyse bilişim sistemi kavramı, fiziki donanımlar ile birlikte mutlaka sistemlerde işlenmek için durağan halde mevcut olan yahut sistemler arasında akan verileri de kapsayacak şekilde, bunların ayrılmaz bir bütünlüğü olarak anlaşılmalıdır.

Bilişim sistemlerinin veriler üzerindeki bu işlemleri gerçekleştirebilmesi için evvela fiziki bir yapı gerekir. İkinci olarak, sistemin somut ve fiziki madde halindeki elementlerine bu yeteneği sağlayacak olan soyut bir unsur daha gerekmektedir. Bu ikili yapılanmada demir, silikon, plastik ve benzeri maddelerin birleşimi olan ve elektrik yahut sair bir enerji ile çalışan fiziki bütünlükler ‘’donanım‘’ olarak adlandırılır.[25] Sistemin veriler üzerinde çeşitli işlemler yapabilme yeteneğine sahip olması için gerekli olan ve sistemdeki çipler ve depolama ünitelerine yüklü verilerden oluşan

[24] Metin TURAN (2019), *Bilişim Hukuku*, Üçüncü Basım, Seçkin, Ankara, s. 49.
[25] Kapsayıcı bir tanım olmasa da mevzuatımızda donanımın tanımı, Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği md. 3/1-e'de ‘’*Elektronik haberleşme altyapısı, bilgisayarlar, veri kaydetmek için kullanılan taşınabilir veya sabit diskleri*‘’ şeklinde yapılmıştır.

soyut unsur ise ‘’yazılım‘’ olarak adlandırılır.[26] Bu yazılımlardan sistemin çalışabilmesi için gerekli olanları, üreticiler tarafından cihazlara gömülü biçimde ve salt okunur(*belirli sınırlar haricinde değiştirilemez*) vaziyette bulunur(*örn. BIOS*). Değiştirilebilen yazılımlardan; bilişim sisteminin hangi esaslar dahilinde çalışacağını belirleyen ve başlıca fonksiyonları yerine getiren yazılımlara sistem yazılımı(*işletim sistemi*), bu temel yazılım haricinde sisteme yüklü olan ve çeşitli alt seviye işlemleri yerine getiren yazılımlara ise uygulama yazılımı denilir.[27]

Yukarıdaki açıklamaları örneklemek gerekirse, bir masaüstü bilgisayarda ekran, kasa, fare ve klavye; elektrik, pil ve sair enerji ile çalışan elektronik donanımlardır. Bunlar genellikle bir veri işleme ve depolama ünitesine sahip değildir. Ana kart/işlemci/CPU, ekran kartı/grafik işlemci/GPU ve depolama üniteleri ise verileri işleme ve depolama faaliyetlerini yerine getiren donanımlardır. Veri depolama faaliyetini yerine getiren donanımlar içerisinde yüklü olan, verileri işleme faaliyetini yerine getiren donanımlar sayesinde çalıştırılabilen/işlenen ve veriler üzerinde çeşitli işlemler gerçekleştirebilmeyi sağlayan ‘’belirli bir amaç doğrultusunda çalışan‘’ veri bütünlükleri ise yazılımları oluşturmaktadır.[28]

2.1.1.2. Network/Ağ ve İnternet

Bilişim sistemleri, bu nitelemeye sahip tek bir donanımdan oluşabileceği gibi tekil bir cihazın, içeriğindeki birden çok gömülü bilişim sisteminden müteşekkil olarak meydana gelmesi de mümkündür. Birden çok sistemden meydana gelen bir bilişim sistemi içerisindeki sistemler kendi aralarında iletişim kurduklarından, bu yapı aynı zamanda dar manalı bir network/ağ yapısını oluşturur. Her türlü bilişim sisteminin bir diğeri ile çeşitli bağlantı teknolojileri vasıtasıyla kablolu/kablosuz altyapılar üzerinden bağlantı sağlaması ve iletişim kurması ise gerçek anlamda bir network/ağ yapısını teşkil eder. Bir ağ yapısının başka bir ağ yapısıyla kurduğu bağlantı ve iletişimler de daha geniş bir ağ yapısını oluşturacaktır.

---

[26] 4691 s. Teknoloji Geliştirme Bölgeleri Kanunu md. 3/1-l’de yazılım, ‘’*Bir bilgisayar, iletişim cihazı veya bilgi teknolojilerine dayalı bir diğer cihazın çalışmasını ve kendisine verilen verilerle ilgili gereken işlemleri yapmasını sağlayan komutlar dizisinin veya programların ve bunların kod listesini, işletim ve kullanım kılavuzlarını da içeren belgelerin, belli bir sistematik içinde, tasarlama, geliştirme şeklindeki ürün ve hizmetlerin tümü ile bu ürün ya da mal ve hizmetlerin lisanslama, kiralama ve tüm hakları ile devretme gibi teslim şekillerinin tümü*‘’ şeklinde tanımlanmıştır.

[27] Nurettin TOPALOĞLU (2014), ‘’Bilgisayar Mimarisi‘’, İçinde, *Adli Bilişim ve Elektronik Deliller*, Ed. Hüseyin Çakır, Mehmet Serkan Kılıç, ss. 25-92, Seçkin, Ankara, s. 25, 56.

[28] Hukuk doktrininde de yazılımlar, veri kavramının bir alt unsuru olarak değerlendirilmektedir. Bu konuda bkz. Berrin AKBULUT 2017, age. s. 14

Bilişim sistemlerinin birbirleriyle yaptıkları bağlantılardan oluşan ağ yapıları, nitelikleri ve kapsama alanlarına göre literatürde çeşitli ayrımlara tabi tutulur. Bu ayrımlardan en yaygın olanı, LAN(*yerel alan ağı*), CAN(*kampüs alan ağı*), MAN(*şehir alan ağı*) ve WAN(*geniş alan ağı*) şeklindeki dörtlü ayrımdır. Bu ağ yapıları diğer ağlarla, bu sayede de çeşitli coğrafyalar birbirleri ile bağlanır ve böylece çeşitli elektronik haberleşme teknolojileri vasıtasıyla küresel çapta elektronik haberleşme sağlanır. Ağ yapılarında, salt bağlı sistemler arasında kapalı devre bir iletişim gerçekleştirilebileceği gibi ağ trafiğini filtreleyerek, yalnızca izin verilen istemci ve sunucuların iletişimine olanak sağlayan teknolojiler vasıtasıyla birkaç ağ da birbiri ile kapalı devre bir iletişim sağlayabilir. Örneğin bir işyeri LAN'ındaki ağ teknolojileri, bağlı sistemler salt kendi aralarında veya izin verilen diğer spesifik ağ yapılarındaki sistemler ile iletişim kuracak şekilde yapılandırılabilir. İnternet ise LAN ve diğer küçük çaplı ağ yapılarının meydana getirdiği WAN'ların, küresel olarak birbirine bağlı olduğu ve kamunun kullanımına açık bir ağ yapısıdır. [29]

İnternet ağı; 1900'lerin ortalarında ABD Savunma Bakanlığı'nın(*Department of Defence-DOD*) güvenlik amacıyla geliştirdiği ARPANET projesinin bir ürünüdür. İnternetin oluşum sürecinde evvela ARPANET kapsamında farklı noktalardaki bilişim sistemleri birbirlerine bağlanmış, bu bağlantıyı sırasıyla ABD ve dünyanın geri kalanındaki sistem ve ağlar izlemiş, nihayetinde de internet ağı bugünkü halini almıştır.[30] Yeni bağlantılar vasıtasıyla daimi olarak genişleyen internet ağı ABD Savunma Bakanlığı'nın yarattığı bir teknoloji olduğundan, temelde DOD-TCP/IP standart modelindeki protokol kümeleri kullanılır. İletişimde standart modellerin kullanımı, bilişim sistemlerinin üreticileri ve/veya içeriğindeki sistem yazılımları farklı olsa bile sağlıklı bir iletişim kurulabilmelerini sağlar.[31]

İnternet iletişimi; cihaz/sistemler ve nihayetinde de ağlar arası bir veri trafiğinin işleyişinden oluşur. Bu veri trafiğinde iletişim halindeki sistemler, ''istemci-sunucu'' olarak isimlendirilirler. Bir bilişim teknolojisi olan internet iletişiminde, iletişime konu verileri barındıran ve bu verileri çalıştıran sunucular bulunur. Bu yapıda evvela veri

[29] Cebrail TAŞKIN (2018)*, Ağ Teknolojileri ve Telekomünikasyon,* Pusula, İstanbul,. s. 23, 24, 27, 28, 29 vd.
[30] DARPA, ARPANET, https://www.darpa.mil/attachments/ARPANET_final.pdf, (ET:02.03.2022), s. 2, 3; Barry M. LEINER, Vinton G. CERF, David D. CLARK, Robert E. KAHN, Leonard KLEINROCK, Daniel C. LYNCH, Jon POSTEL, Larry G. ROBERTS ve Stephen WOLF (1997), *Brief History of The Internet*, Internet Society, s. 3, 4, 5 vd.
[31] Toros Rifat ÇÖLKESEN (2018), *Network-TCP/IP-UNIX*, Onbirinci Basım, PapatyaBilim, İstanbul, s. 75.

dosyalarının barındırıldığı ‘’veri tabanı sunucular‘’ yer alır. İnternet teknolojilerinde verilerin istemci-sunucu arasında iletimi ve bunların front-end(*ön yüz*) tarafında kullanıcılar, back-end(*arka yüz*) tarafında geliştiriciler yönünden algılanabilmesi için çeşitli protokoller, yazılımlar ve programlama dilleri faaliyettedir. Bu faaliyetleri gerçekleştiren verileri barındıran/çalıştıran ve veri tabanı ile aradaki bağlantıyı sağlayan ise uygulama sunucularıdır.[32] İnternet iletişiminde bu sunucular vasıtasıyla iletişim kuran sistemler eğer aynı zamanda iletişimde sunucu taraf değilse, literatürde ‘’istemci‘’ olarak adlandırılırlar.[33]

İnternet iletişiminin sağlanması için gerekli olan[34] TCP/IP protokoller kümesinin işleyişinde istemci ve sunucuların statik ya da dinamik IP adresleri bulunur. Sunucuların parçalara bölünmesi(*sanallaştırma*) mümkün olduğundan, sunucuların birden çok IP adresi bulunabilir.[35] İnternet ağına/WAN’a çıkış yapacak sistemler, bu bağlantıyı gerçekleştiren modem/router vasıtasıyla erişim sağlayıcının omurgasına ve routerlarına erişirler. Bu sebeple IP adreslerini erişim sağlayıcılar atar ve yerel ağdaki sistemler, internete erişim sağlayıcıların atadığı bu IP adresleri ile çıkış yaparlar.[36] Bu IP adresleri internet ağında sistemlerin birbirleri ile sağlıklı iletişim kurabilmesini sağlamanın ilk aşamasıdır. Bu iletişimin sağlıklı biçimde tamamlanması için yerel

---

[32] Gökhan USTA (2019), *Ethical Hacking(Hacking Kursu)*, Seçkin, Ankara, s. 114, 115, 116 vd. / Site/uygulamanın işleyişi için kullanılan yazılımlar farklı sunucularda veya tek bir sunucunun farklı sanal bölümlerinde barındırıldığı zaman uygulama sunucusu-veri tabanı sunucusu ayrımı yapılabilir ise de bu iki katmanın tek sunucu içerisinde işletilmesi de pekala mümkündür. / İstemci-sunucu arasındaki iletişimde bu veri tabanı-uygulama sunucusu ayrımı aynı zamanda site/uygulamanın katmanlarını da teşkil etmektedir. / İnternet uygulamaları ve sitelerinin sunucular vasıtasıyla işleyişinde üç katman bulunduğu ve bunların sunucu katmanı, orta katman ve back-end/arka uç olduğu yönünde görüşler de mevcuttur. Bu yönde bkz. Bünyamin DEMİR (2020), *Yazılım Güvenliği(Saldırı ve Savunma)*, Dikeyeksen, İstanbul, s. 14.

[33] Wikipedia, İstemci, https://tr.wikipedia.org/wiki/%C4%B0stemci, (ET: 02.03.2022); Wikipedia, Sunucu, https://tr.wikipedia.org/wiki/Sunucu_(bili%C5%9Fim), (ET: 02.03.2022).

[34] Hüseyin POLAT (2014), ‘’Bilgisayar Ağları ve Adli Bilişim‘’, İçinde, *Adli Bilişim ve Elektronik Deliller*, Ed. Hüseyin Çakır, Mehmet Serkan Kılıç, ss. 96-136, Seçkin, Ankara, s. 101, 106.

[35] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik md. 3/1-h’de IP adresi şu şekilde tanımlanmaktadır: ‘’*Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adres*‘’. Web sunucularda belirli zaman aralığı için statik IP atanması olağan olup, DNS sisteminin geleneksel işleyişi için bu durum idealdir. Ancak dinamik DNS teknolojileri ile DNS sunucularına alan adına dair IP değişikliğinin belirli programlar vasıtasıyla iletimi mümkün olup, dinamik IP’ler üzerinden de sunucu yayını yapılması mümkündür. Başta P2P sistemler olmak üzere, sistemlerin hem istemci hem sunucu olarak görev yapabileceği(*örneğin kişinin kendi bilgisayarını aynı zamanda web sunucu olarak çalıştırması*) durumlarda dinamik IP’ler üzerinden yayın yapılması gündeme gelebilmektedir. Böyle bir düzende kullanıcıların İSS’lerden statik IP adresi edinmeleri mümkün olmakla birlikte, zorunlu değildir.

[36] Belirtmek gerekir ki LAN sanallaştırılıp parçalandığında ortaya çıkan VLAN’lar arasındaki ve ayrı VLAN’lardaki sistemlerin iletişimi ve WAN’a çıkışı için farklı sanal routerlar oluşturulabilir. Ancak temelde iki ayrı fiziki router ve iki ayrı ağ aboneliği veya tek abonelikten kaynaklı birden çok atanmış IP adresi yoksa, internete çıkış IP’si erişim sağlayıcının atadığı IP adresi olacaktır.

ağda da modem ve ağa bağlı diğer sistemler arasındaki iletişimin düzgün işlemesi gerekir. Bu sebeple yerel ağdaki her bir sisteme/cihaza modem/router veya NAT protokolü ve DHCP'yi işletecek sair cihazlar tarafından, yerel ağ içindeki iletişimde kullanılacak olan ve erişim sağlayıcıların atadığı IP adreslerinden farklı olarak ''*LAN IP adresleri*'' atanır. İnternetteki veri trafiğinde pek çok farklı noktada pek çok farklı işlem ve veri alış-verişi gerçekleştiğinden, bu çok sayıdaki farklı veri alış-verişini sağlaması ve farklı iletişimlerin birbiriyle karışmaması için sistemlerde pek çok sanal port bulunur. Bu şekilde belirli port/iletişim kanalları üzerinden akan veri trafiğinde veriler hem IP hem de ilgili portlar vasıtasıyla akar.[37]

Bir LAN içerisindeki sistemlerin internet trafiğinin haricinde salt iç ağda yaptıkları iletişim bakımından ise temelde MAC adresleri kullanılır. Ağ bağlantısı kurabilen sistemlerde, ağ iletişimine yarayan bir Ethernet noktası/kartı/portu bulunur. Fiziki bir yapıda olan Ethernet noktalarına üretici firmalar benzersiz birer kod işleyerek bunları kimliklendirirler. İşte bu kimlik, ağ iletişimi kurabilen sistemin MAC adresi olarak adlandırılmaktadır.

2.1.1.3. Veri ve Siber Uzay

Yirmi yıldan daha uzun bir süre önce oluşturulan ASS'de bilişim yerine doğrudan bilgisayar kavramı kullanılmıştır.[38] Sözleşmede bilgisayar verisi,

---

[37] ''*Günümüzde kullanılan işletim sistemleri çok sayıda programın aynı anda çalışmasına izin vermektedir. Kullanılan programlardan bazıları bilgisayara dışarıdan gelen istekleri (istemci / istek) kabul etmekte ve uygun istekleri de cevaplamaktadır (sunucu / cevap). Bu istek cevap olayını bilgisayarlar üzerinde yapmak için birtakım soyut bağlantı noktaları tanımlanır ve adresleme yapabilmek adına pozitif bir sayı verilir, bu sayılar port numaralarıdır*.'' Mustafa Yasir ŞENTÜRK (2018), *Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinden Uygulanması*, Türk Hava Kurumu Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Ankara, s. 34; ''*Bilgisayar ağlarında , bir bağlantı noktası bir iletişim uç noktasıdır. Yazılım düzeyinde, bir işletim sistemi içinde, bağlantı noktası, belirli bir işlemi veya bir ağ hizmeti türünü tanımlayan mantıksal bir yapıdır . Her aktarım protokolü ve adres kombinasyonu için bağlantı noktası numarası olarak bilinen 16 bitlik işaretsiz bir sayı ile bir bağlantı noktası tanımlanır . Bağlantı noktası numaralarını kullanan en yaygın aktarım protokolleri, İletim Denetimi Protokolü (TCP) ve Kullanıcı Veri Birimi Protokolü'dür (UDP). Bir bağlantı noktası numarası her zaman bir ana bilgisayarın IP adresi ve iletişim için kullanılan aktarım protokolünün türü ile ilişkilendirilir. Bir mesajın hedef veya başlangıç ağ adresini tamamlar. Gelen bir paketin çalışan bir uygulamaya kolayca iletilebilmesi için belirli hizmetleri tanımlamak için belirli bağlantı noktası numaraları ayrılmıştır. Bu amaçla, 1024'ten küçük bağlantı noktası numaraları, geçmişte en sık kullanılan hizmetleri tanımlar ve iyi bilinen bağlantı noktası numaraları olarak adlandırılır . Uygulamalar tarafından genel kullanım için daha yüksek numaralı bağlantı noktaları mevcuttur ve geçici bağlantı noktaları olarak bilinir*.'', Wikipedia, Port, https://en.wikipedia.org/wiki/Port_(computer_networking), (ET: 02.03.2022).

[38] Aşağıda ASS'nin bilgisayar kavramı ile genel olarak bilişim sistemlerini kastettiği açıklanmıştır. Bu sebeple ASS'de geçen ''bilgisayar verisi'' kavramının da bilişim verisi şeklinde anlaşılması doğru olacaktır.

''*bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsili*''

şeklinde tanımlanmıştır. Sözleşmenin açıklayıcı raporunda ise ilgili kavram, *bilgisayar/bilişim sistemlerinin otomatik olarak işleyebildiği ve işlenmeye uygun haldeki elektronik ve diğer biçimlerdeki veriler* şeklinde açıklanmaktadır.[39]

5651 s. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[40] ve bağlı alt mevzuatta veri, ''*Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*'' şeklinde tanımlanmıştır.[41] Ayrıca Mesafeli Sözleşmeler Yönetmeliği md. 4/1-a'da, bilişim verilerinin bir araya gelerek oluşturduğu veri toplulukları ''dijital içerik'' olarak adlandırılmış ve ''*Bilgisayar programı, uygulama, oyun, müzik, video ve metin gibi dijital şekilde sunulan her türlü veri*'' şeklinde tanımlanmıştır. TCK md. 243'ün gerekçesinde ise ''*Sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır.*'' denilmektedir. Doktrinde yer alan tanımlardan, verinin olması gereken bir tanımına örnek olarak ise şu tanım verilebilir:

''*Bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi*''[42]

Doktrinde bilgi, ''… *verinin bir üst formu olup, verinin değerlendirilmiş, analiz edilmiş, düzenlenmiş ve verinin belirli bir anlam ifade edecek forma dönüştürülmüş halidir. …*'' şeklinde tanımlanmaktadır.[43] Bu şekliyle bilgi kavramı, verilerin bilişim sistemlerinin ekranlarında görülen veya hoparlörlerinden duyulan şekilleri ile aynı anlama gelmemektedir. Bu kullanımıyla bilgi, istatistiki olarak veriler üzerinde yapılan çalışmalardan üretilen anlamlı sonuçlar ile ilgilidir. Ancak aynı zamanda veriler, bilişim sistemlerinde çalışan/işlenen (*verilerden oluşan*)yazılımlar ve

[39] ASS Açıklayıcı Raporu, https://rm.coe.int/16800cce5b, (ET: 02.03.2022).
[40] Yayımlandığı Resmî Gazete: Tarih: 23/5/2007 Sayı: 26530
[41] İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun md. 2/1-k; İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik md. 3/1-p; Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik md. 3/1-s.
[42] Murat Volkan DÜLGER 2022, age. s. 80.
[43] Şeref SAĞIROĞLU (2018), ''Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler'', İçinde*, BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 1, Siber Güvenlik ve Savunma-Farkındalık ve Caydırıcılık*, Ed. Şeref Sağıroğlu, Mustafa Alkan, ss. 21-45, Grafiker, Ankara, s. 22, 23 / Benzer tanımlama için bkz. Onur KORUCU (2021), *Veri Güvenliğinin İyileştirilmesi Sürecinde Küresel Standart, Çerçeve ve En İyi Uygulamaların Hukuki Uyuma Desteği*, Adalet, Ankara, s. 23, 24.

donanımların birlikte çalışması sonucunda, insanın duyu organları tarafından algılanabilecek anlamlı sonuçlar doğururlar. Şüphesiz ki bu sonuçlar da ‘’bilgi‘’ olarak adlandırabilir ve pratikte de bu kullanım mevcuttur. Mevzuatımızda(*5651 s. Kanun*) ‘’*verilerin anlam kazanmış biçimi*‘’ şeklinde açıklanan bilgi kavramı da kanaatimizce bu yöndedir.

Evrendeki tüm bilişim sistemlerinin ve gerek bu sistemlerin içerisindeki gerekse sistemler arasında akışta olan verilerin külli toplamı ise siber uzay olarak adlandırılır.[44] Bazı görüşlere göre ise siber uzay, çeşitli ağ bağlantıları vasıtasıyla birbirlerine bağlı bilişim sistemlerinin oluşturduğu ağı ifade eder.[45] Ancak esasında siber uzay yalnızca ağlar veya ağ yapılarına ait fiziksel bileşenler ile ilgili bir kavram değildir. Siber uzay kavramı, durağan halde ya da akış halinde bulunan bilişim verilerinden müteşekkil soyut bir alandır.[46]

Yukarıdaki açıklama ve tanımlamalardan ortaya çıkan sonuç, verilerin evvela bilişim sistemleri içerisindeki (*veri işleyen ve/veya depolayan*)donanımlar içerisinde ve ikinci olarak da ağ yapılarında akış halinde bulunduğudur. Ayrıca veriler değiştirilebilir, silinebilir veya aktarılabilir oldukları için bilişim sistemlerinden ayrı bir değere sahip olduklarını belirtmek gerekir. Lakin bir bilişim sistemini verilerden bağımsız olarak düşünmek mümkün olmadığından bilişim sistemleri, içlerindeki verilerden/siber uzaydan ayrı bir değer ifade edemez.

2.1.1.4. IoT, M2M ve Akıllı Cihaz Teknolojileri

Günümüzde neredeyse bütün aletlerin mekanik hale getirilmesi ve bilahare bu aletlere içerisinde yazılımların yüklü olduğu Arduino vb. kartlar[47] yahut sair gömülü

---

[44] Ulaştırma ve Altyapı Bakanlığı 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı’nda siber uzay, ‘’*Tüm dünya ve uzaya yayılmış bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam*‘’ şeklinde tanımlanmıştır. Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik md. 4/1-ç’de ise ‘’sanal ortam’’ olarak isimlendirilen, ‘’*Bilgisayar, internet, interaktif televizyon, cep telefonu ve benzeri bilişim ortamları …*‘’ şeklinde bir tanım mevcuttur.

[45] ‘’*Dünyada milyonlarca insan, bilgisayar, tablet bilgisayar, akıllı telefon, akıllı televizyon, oyun konsolu ve Internet of Things-IoT (internet cihazları) vb. cihazlar ile birbirine internet aracılığıyla bağlı durumdadırlar. Bu birbirine bağlı cihazların oluşturduğu ağı kısaca siber uzay olarak da adlandırmak mümkündür.*‘’ Eyüp TEKİN (2017), *Adli Bilişimde Açık Kaynak Kullanımı*, Polis Akademisi Adli Bilimler Enstitüsü Kriminalistik Anabilim Dalı Yüksek Lisans Tezi, Ankara, s. 1.

[46] Semih Töner ŞEN (2021), *Siber Uzay ve Uluslararası Hukuk*, Oniki Levha, İstanbul, s. 5, 6, 7 vd.

[47] Arduino kartlar(*örn. UNO*), veri işleme/depolama olanağına sahip bir mikro denetleyici çip ve bu çipe ekli olarak USB, Ethernet ve sair port ünitelerinin, ek depolama ünitelerinin ve sair birimlerin yer aldığı bilişim sistemleridir. Aynı işlevi yerine getiren Raspberry kartları ve ayrıca Türk üretimi Deneyap Kart sistemleri de mevcuttur. Yazılımlara sahip bu kartlar portları, Ethernet ve sair bağlantı noktaları vasıtasıyla bağlandığı bilgisayar ve benzeri cihaz üzerinden programlandığı zaman, temelde bir akıllı cihazda veya akıllı cihaz ağlarındaki çeşitli işlevleri yerine getirmek için diğer cihazlar içerisinde

sistem/çipler yerleştirilerek, bunların birer bilişim sistemine dönüştürülmesi mümkündür. Bu şekilde bir fotoğraf makinesi, buz dolabı veya basit bir aynanın, içerisindeki gömülü sistemler vasıtasıyla verileri işlemesi, depolaması ve/veya aktarması yahut veriler üzerinde sair işlemler gerçekleştirmesi olanak dahilinde olmaktadır. Bu tür bilişim sistemleri, temel olarak akıllı cihaz teknolojilerini oluşturur.[48]

Akıllı cihazlardaki bu gömülü sistemlere ağ bağlantı teknolojileri olan Ethernet girişleri(*Network Interface Card*), sim kart yuvaları, Bluetooth veya sair birimler eklendiğinde ise bu sistemler diğer bilişim sistemleri ile iletişim kurabilir ve ağ bağlantısı sağlayabilir hale gelirler. Örneğin bir evde ısıyı, temizliği, güvenliği ve aydınlatmayı kontrol eden sistemler birbirine ve nihayetinde de ev sahibi ve/veya sistemleri kontrol eden firmanın bilgisayar/telefon ve sair sistemine bağlı olarak çalışabilir. İşte bu bilişim sistemi ağlarına yani makineden makineye iletişim teknolojisine, temel olarak Machine to Machine/M2M denilmektedir.[49]

M2M teknolojilerinde iletişim, yukarıda zikredildiği üzere çok farklı ağ teknolojileri vasıtasıyla işleyebilir. Eğer bu teknoloji internet altyapısı üzerinden işliyor ve örneğin sim kartlar + baz istasyonları veya alıcılar + uydular veya Ethernet port/wi-fi + fiber altyapı kullanılarak M2M sistemler birbirleri ile iletişim kuruyor ise bu teknoloji bir yönüyle Internet of Things/IoT(*nesnelerin interneti*) kavramına karşılık gelir. Ancak IoT temelde internet altyapısını kullanan akıllı cihazların çok ötesinde, M2M gibi her türlü alt yapıyı kullanabilen, M2M'den çok daha büyük ağ yapıları içerisinde akıllı cihazların iki nokta arasında değil de çok eşli biçimde ve sınırlı bir insan müdahalesi dahi olmaksızın her türlü kullanıcı tipi yönünden kendi kendilerine iletişim kurabilmeleri ve belirli görevleri yapabilmeleri anlamına gelen bir kavramdır. Örneğin iki internet kullanıcısı haberleşirken, bilişim sistemlerini fiilen kullanırlar. Bir fabrikadaki IoT makineler ise insanların fiili kullanımı olmadan birbirleriyle iletişim kurarak üretim faaliyetlerine katılabilirler ve işlerini yapabilmeleri için devamlı olarak insanların komutlarına ya da insan vasıtasıyla birbirleri arasında bir bağlantı sağlamalarına ihtiyaç duymazlar.[50] Beşinci jenerasyon

kullanılır. Bu kartlar M2M sistemlerde gömülü sistemler içerisinde kullanılabileceği gibi gerekli donanımlar ile bağlandığında ve amaca göre programlandığında, temel bir bilgisayarın yapabileceği çoğu işlevi de yerine getirebilir.

[48] Wikipedia, Smart Device, https://en.wikipedia.org/wiki/Smart_device, (ET: 02.03.2022).

[49] Wikipedia, M2M, https://en.wikipedia.org/wiki/Machine_to_machine, (ET: 02.03.2022).

[50] Wikipedia, Internet of Things, https://en.wikipedia.org/wiki/Internet_of_things, (ET: 02.03.2022); Sorting Out The Difference Between M2M and IoT, https://blog.parker.com/site/usa/en-US/details-

mobil ağ bağlantısı iletişim teknolojilerinin(*5G*) hayata geçmesi ve IoT sistemlerin daha da yaygınlaştığı ve entegre biçimde çalıştığı yapıya, toplum 5.0 denilmektedir.[51]

Klasik bilişim sistemleri ile M2M/IoT teknolojileri arasındaki ilişki de önem arz eden bir husustur. Bilişim verileri üzerinde işlem gerçekleştirebilme kabiliyetine sahip sistemlerin ve/veya bunlar üzerindeki gömülü sistemlerin bilişim sistemi niteliğinde olduğu göz önünde bulundurulursa, her bir M2M/IoT sistemi birer bilişim sistemi olarak kabul edilecektir. Ancak her bilişim sistemi M2M/IoT kavramlarına dahil olmayıp, bu kavramlar içerisine yalnızca bilişim sistemleriyle iletişim kurabilir hale getirilmiş yeni nesil akıllı cihaz teknolojileri dahil edilir. Örneğin çok uzun süredir ağ yapıları içerisinde bilişim sistemleriyle iletişim kuran masa üstü bilgisayarlar M2M/IoT kavramlarına dahil edilmez.[52] Bu kavramlar daha çok onlara bilişim verileri üzerinde işlemler gerçekleştirme yeteneğini kazandıran gömülü sistemleri olmaksızın geçmişte ve günümüzde genel olarak kullanılan ancak genel kullanımında bilişim teknolojilerinin alanına girmeyen fırın, kamera, klima veya sanayide kullanılan makineler için kullanılır.

Akıllı cihazların içerisindeki gömülü sistemleri vasıtasıyla internet, kızılötesi, bluetooth, NFC, Zigbee ve sair ağ iletişim teknolojileri vasıtasıyla iletişim kurdukları M2M/IoT teknolojileri, iletişimde kullanılan alt yapı farklılıkları ve türlerin sayısal fazlalığı sebebiyle, birbirleriyle bilgisayar ya da telefon türlerindeki kadar yapısal bir benzerlik göstermezler. Bu sebeple klasik bilişim sistemlerindeki TCP/IP-DOD veya OSI standart modeli gibi bir standartlaşma, IoT sistemlerde henüz ortaya çıkamamıştır[53] Doktrinde IoT sistemlerin yapısal modellemelerinde genel olarak üç ve beş katmanlı mimarinin tercih edildiği belirtilir. Üç katmanlı modelde algılama, ağ ve uygulama katmanı bulunur. Beş katmanlı modelde ise algılama, ağ, işleme, uygulama

---

home-page/sorting-out-the-difference-between-m2m-and-iot-usi (ET: 02.03.2022); Hasan ÖZKÖSE (2014), *Makineler Arası Haberleşme (M2M) ve Türkiye İçin Düzenleyici Öneriler*, Bilgi Teknolojileri ve İletişim Kurumu Bilişim Uzmanlığı Tezi, Ankara, s. 1,2,3,4,5 vd.; Cebrail TAŞKIN 2018, age. s. 334, 335; Şeref SAĞIROĞLU (2019), ‘’Siber Güvenlik ve Ötesi‘’, İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 2, Siber Güvenlik ve Savunma-Problemler ve Çözümler*, Ed. Şeref Sağıroğlu, Mustafa Şenol, ss. 25-60, Grafiker, Ankara, s. 47, 48; Emrah YETİMLER, *İnternet of Things(Nesnelerin İnterneti) Nedir? Cihazların Etkileşim Trendleri,* Aktaran: Armağan Ebru Bozkurt YÜKSEL (2021), ‘’Nesnelerin İnternetinin Hukuki Yönden İncelenmesi‘’, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* C. 17, S. 2, ss. 113-139, s. 116; Dijital Türkiye Platformu (2021), *Dijitalleşme Yolunda Türkiye*, https://assets.kpmg/content/dam/kpmg/tr/pdf/2021/04/dijitallesme-yolunda-turkiye-raporu-2021.pdf, (ET: 02.03.2022), s. 33.

[51] Dijital Türkiye Platformu, age. s. 8.

[52] Wikipedia, M2M

[53] Füsun Yavuzer ASLAN (2020), *Nesnelerin İnterneti Uygulamalarının Güvenliği İçin Hafif Sikler Kriptografik Algoritmaların Analizi ve Güvenli Akıllı Bir Platform Uygulaması*, Trakya Üniversitesi Fen Bilişimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Doktora Tezi, Edirne, s. 9, 19.

ve iş katmanları yer alır. İşte akıllı cihazları veriler üzerinde işlem gerçekleştirme kabiliyetine kavuşturarak, bunları birer bilişim sistemi haline getiren şey, bu katmanlardaki yazılım ve donanım birleşimleridir. Bu katmanlardaki çiplerin, sensörlerin, ağ bağlantısı ve veri depolama üniteleri ile sair unsurların işleyişi sayesinde bu akıllı cihazlar bilişim verileri üzerinde çeşitli işlemler gerçekleştirmektedirler.[54] Öyleyse M2M/IoT cihaz/sistemlerde ‘’bilişim sistemi‘’ sıfatının esas olarak bir klimaya ya da endüstriyel robota değil, bunlar üzerindeki bilişim sistemlerinin birlikte işlemesinden ortaya çıkan yapıya yahut en nihayetinde içerisindeki gömülü sistemlere ait olması gerektiğini söylemek mümkündür.[55]

2.1.2. Alt Kavramlar Işığında Bilişim Sistemi Kavramının Açıklanması

2.1.2.1. Bilişim Sistemlerinin Sıralanması

Bir teknolojik yapıya bilişim sistemi vasfını kazandıran, veriler üzerinde çeşitli işlemleri yapabilme kabiliyetidir. Günümüzde bu kabiliyete sahip olan pek çok sistem ve bu sistemlerin birlikte işlediği daha kapsamlı sistemler mevcuttur. Çok sayıdaki farklı türde bilişim sistemleri yönünden yapılabilecek bir sıralama, temelde akıllı cihazlar ve sair cihazların veriler üzerinde işlem gerçekleştirme kapasitesine sahip ve içeriğinde kök yazılımları barındıran ‘’gömülü sistemlerinden‘’ başlatılabilir. Bu gömülü sistemlerden bir adım ötede; işlemcisi, belleği/veri depolama ünitesi ve farklı işlevleri yerine getiren bağlantı portları bulunan Arduino ve Raspberry gibi mikro denetleyici kartlar veya diğer bir isimlendirme ile ‘’tek kart bilgisayarlar‘’ konumlandırılabilir.

Bilişim sistemlerinin sıralanmasında başlangıç noktası/zemini mikro işlemciler ve mikro denetleyiciler olarak alındığında, bunların yalnız başına veya sair benzerleriyle birlikte kullanılmasıyla yapılandırılan ‘’akıllı cihazlar‘’, sıralamanın ilk basamağında bulunabilir. Bu noktada akıllı ev aletleri, akıllı saatler, IP kameralar, akıllı kilitler veya endüstriyel kullanımdaki aletlere yer vermek uygun olacaktır. Burada önemli olan konu, yalnızca belirli bir veya birkaç işlevi yerine getirmesi için tasarlanan bu tür akıllı cihazların, tasarımları geliştirilerek ve donanımlarına ve/veya

[54] Füsun Yavuzer ASLAN 2020, age. s. 10,11,12

[55] Bu yapılarda birden fazla gömülü sistem veya veriler üzerinde işlem gerçekleştirme kabiliyetine sahip birimler birlikte çalışmıyorsa, en temelde bunların mikro işlemcilerinin bilişim sistemi sayılması gerektiği yönünde benzer görüşler için bkz. Burak Cesur AKÖZ (2018), *Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları ile Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri*, Bilgi Teknolojileri ve İletişim Kurumu Bilişim Uzmanlığı Tezi, Ankara, s. 14.

yazılımlarına ufak eklemeler yapılarak bir tablet bilgisayar ile aynı işlevi yerine getirebileceği olgusudur. Bu yöndeki en basit örnek akıllı saatlerdir. Tıpkı IP kameralar gibi ağ bağlantı çıkışları ve veri işleme, depolama, aktarma birimleri bulunan temel bir akıllı saatin Android-İOS ve benzeri işletim sistemi bulunmakta, bunlar ile bir tabletin yapabileceği her şey yapılabilmektedir. Şüphesiz ki bir IP kamera için de aynı geliştirmenin yapılabilmesi mümkündür. Bu sebeple sıralamanın bu noktasında bir bilgisayar ile benzer işlevleri yerine getirebilen ve örneğin Youtube'a girilebilen bir saatin değil, yalnızca belirli birkaç işlevi yerine getirebilen akıllı saatlerin yer alması doğru olacaktır. Yukarıda zikredildiği üzere bu tür akıllı cihazlar, üzerlerindeki ağ bağlantısı noktaları vasıtasıyla M2M/IoT bilişim sistemleri vasfı kazanır ve diğer bilişim sistemleriyle haberleşirler.

Bu ''ilk basamak'' seviyedeki bilişim sistemlerini, tez konusu TCK md. 243 ile bağlantılı şekilde açıklayacak bir örneklendirmenin, veri işleme ve aktarma sağlayan mikro işlemciye(*ya da birlikte çalışan işlemci+belleğe*) ve kablosuz Ethernet portuna/wi-fi kartına sahip bir akıllı kilit sistemi üzerinden yapılması mümkündür. Evdeki bağlantı noktası üzerinden wi-fi teknolojisi ile kablosuz LAN'a bağlı bir akıllı kilit, çok çeşitli yöntemler ile hacklenebilir. MAC adresine ve modemin atadığı iç IP adresine sahip olan bu kilidin, ufak bir SD kart ile depolama ünitesi bulunabilir ve burada kilit sisteminin ne zaman ve kim(*hangi token-parmak izi ve sair kullanıldı-hangi MAC adresine sahip istemci kilidi uzaktan açtı vb.*) tarafından açılıp kapatıldığına dair loglar tutulabilir. Eğer kilit sisteminin parolaların girildiği ve sair işlemlerin yapılabildiği bir ekranı bulunuyor ve bu ekran aynı zamanda SD içindeki verilere de erişme imkanı sunuyorsa, bu takdirde parolayı bilen ya da kıran biri yetkisiz biçimde fiziksel olarak bilişim sistemine yetkisiz erişim gerçekleştirebilir. İkinci olarak bu sistemin ekranı bulunsun veya bulunmasın, ağ üzerinden gerçekleştirilecek fiiller vasıtasıyla da bilişim sistemine yetkisiz olarak erişilebilir.[56]

İkinci basamakta ise klasik harici veri depolama-aktarma üniteleri olan SD, USB, CD, hard disk ve benzerleri, üçüncü basamakta ise NAS gibi bunların gelişmiş biçimleri ya da çok fonksiyonlu gelişmiş yazıcılar örnek olarak verilebilir. Yine bu basamaklardan birine modem, router, switch gibi network cihazları ile omurgadaki gelişmiş versiyonları da dahil edilebilir. Bilişim sistemlerine dair yaptığımız sübjektif

[56] Akıllı kilitlerin hacklenmesi ve bu sistemlerdeki BLE iletişim mimarisi ile veri iletişimine dair ayrıntılı anlatılmar için bkz. Besim ALTINOK (2021), *Kablosuz Ağ Güvenliği(Saldırı-Savunma-Analiz),* Üçüncü Basım, Abaküs, İstanbul, s. 186, 187, 188, 189, 190, 191, 192, 196 vd.

sıralamanın son basamağında ise veriler üzerinde genellikle her türlü işlemi yapabilen, içerisinde çok farklı yazılımların çalıştırılabildiği gelişmiş üst seviye bilişim sistemleri konumlandırılabilir. Bunlar Youtube'a erişilen, Tweet atılabilen akıllı saatlerden başlayarak; akıllı telefonlar, tabletler, oyun konsolları, akıllı televizyonlar, sunucular ve pekala bilgisayarların dahil edileceği bir seviyedeki sistemlerdir. Farklı bir basamakta konumlandırılamayacak olan ve niteliği ne olursa olsun bilişim sistemlerinin birbirleriyle oluşturdukları bağlantılardan meydana gelen ağ yapıları ve bu ağ yapılarının birbirleriyle yaptıkları bağlantılardan meydana gelen daha kapsamlı sair ağ yapıları da şüphesiz ki bilişim sistemi niteliğindedir.

2.1.2.2. Bilişim Sistemi Kavramının Fiziksel ve Soyut Unsurların Ayrılmaz Bir Bütünlüğü Olduğu

Bilişim sistemi kavramı, yalnızca veriler üzerinde işlem gerçekleştirilebilmesini sağlayan donanımları niteleyen ya da bunların birleşimi ile oluşturulmuş bilgisayar ve benzeri cihaz için kullanılan bir kavram değildir. Bilişim sistemleri üretilirken, fiziksel parçaların içerisine temel yazılımlar/veriler de yüklenir ve sistem bu şekilde kullanıma sunulur. Örneğin bir bilgisayarın içerisindeki tüm donanımları mevcut olsa bile bu donanımlar üzerinde hiçbir veri bulunmazsa, bu bilgisayar temel işlevlerini dahi yerine getiremeyecektir. Bilişim sistemlerinin temel işlevi ve onlara bu sıfatı kazandıran husus, en dar anlamda verileri işlemektir. Verileri işleyebilen, veriler üzerinde çeşitli işlemler gerçekleştirebilen bir sistemin içerisinde de bu işlemleri gerçekleştirmesini sağlayan, üreticiler tarafından sistemlerdeki mikroçiplere yerleştirilmiş gömülü veriler bulunur ki bu veriler sistemin soyut unsurunu oluştururlar. Örneğin temel görevi depolama birimlerinden aldığı verileri işlemek olan işlemciler, bu depolama birimleri/bellek ile birleşik tasarlanabileceği gibi ayrık tasarlansa bile içlerinde önbellek birimi bulundururlar.[57] Yine işlemciden ayrı konumlandırılan BIOS da dahili belleklerde değil, ana kart üzerindeki bir mikroçipte yüklü bulunur. Öyleyse bilişim sistemi kavramının hem fiziksel bütünlük hem de siber uzay/soyut ortamın ayrılmaz bir bütünü olarak, ''*donanım + yazılım/veri / somut ve soyutun birleşimi*'' şeklinde anlaşılması gerekmektedir.[58]

[57] Wikipedia, *CPU Cache,* https://en.wikipedia.org/wiki/CPU_cache, (ET: 02.03.2022).
[58] Bu sebeple elektronik devreler sayesinde girdiye göre salt belirli çıktılar üreten bir çipin değil, bu çıktıların belirli bir yönde birleştirilerek bir ''veri bütünü'' oluşturması sayesinde ''veri bütününün'' kuralları doğrultusunda sonuçlar üretilmesini sağlayan bir yapının bilişim sistemi sayılması gerekir.

2.1.2.3. Bilişim Sistemi ve Veri Kavramlarının Birbirinden Ayrılması

Bilişim sistemleri ile veriler arasındaki ilişkinin ve farkın anlaşılması önemlidir. Yukarıda bir ağ teknolojisi olarak internetin, verilerin iletimi üzerine kurulu bir mimari olduğu ve iç içe geçmiş irili ufaklı ağ yapılarının bütününden meydana geldiği belirtilmişti. İnternet iletişiminde istemci ve sunucunun arasında sağlıklı bir veri trafiği gerçekleşebilmesi için pek çok bilişim sistemi devreye girer. Temel bir yapıda istemcinin bilgisayarı bağlantı noktasına switch, hub ya da direkt üzerindeki portlar vasıtasıyla bağlanır, bağlantı noktasından omurgaya ve router tarafından erişim sağlayıcı ağına ve WAN'a çıkartılır, WAN üzerinde de araya DNS, Proxy-VPN sunucular ve sair ara cihazların da girmesiyle aynı işlemler daha büyük çaplı olarak tekrarlanarak, bir routerdan ötekine ve çeşitli erişim sağlayıcıların omurgaları üzerinden nihai sunucuya ulaşılır. Bu yapıda internet iletişiminin tecellisi için kullanılan bilgisayar, sunucu, modem ve benzeri sistemler bilişim sistemi sayılırlar. İkinci olarak, bu tekil sistemlerin birlikte oluşturdukları ağ yapıları ve nihayetinde internet omurgası vasıtasıyla meydana getirdikleri daha büyük ağ yapıları da büyükten(*internet=WAN + çok sayıda WAN*) küçüğe(*LAN*) ayrı ayrı bilişim sistemi sıfatını taşıyacaktır.[59] Lakin internet omurgasındaki iletişime dair trafik içerisindeki/nakil halindeki bu veriler, yalnız başına bir bilişim sistemi olarak nitelendirilemez.

Sosyal medya hesapları yahut bulut hesapları gibi kullanıcı ara yüzleri vasıtasıyla erişilen/değiştirilebilir kılınan internet ortamları(*örn: Facebook*) veya e-posta sunucusundaki verilere erişilen e-posta uygulaması(örn. *Outlook*) yahut tarayıcı ile ulaşılan bir e-posta sitesi (örn. *gmail.com*), yer sağlayıcıların sunucular ağında yer alan verilerin bütününün siber uzayda oluşturdukları dijital ortamlardır.[60] İstemci ve sunucu arasındaki iletişimde bu dijital ortamın erişilebilir, görülebilir veya değiştirilebilir olmasını sağlayanlar ise yine verilerden oluşan yazılımlardır. Tüm bu veri toplulukları ise fiziki bütünlüğü olan donanımlar yani veri tabanı sunucuları, uygulama sunucuları ve sair sunucunun içerisinde barındırılmaktadır. İşte Facebook sunucularının birleşerek Facebook.com dijital ortamını meydana getirmelerini

[59] Aynı yönde bkz. Berrin AKBULUT 2017, age. s. 125.

[60] Yargıtay 12. Ceza Dairesi'nin 2015/10388 E. 2017/1556 K. sayılı içtihadında ise bu tür internet ortamlarının da bilişim sistemi olduğu belirtilmiştir. Halbuki bu tür internet ortamları, tekil bilişim sistemleri olan sunucular veya bu sunucuların oluşturduğu ağlarda barındırılan verilerin, kod-yazılım-protokollerin işlemesiyle anlamlandırılmasından ibarettir. Nihayetinde de bunlar bilişim sistemi olan sunucuların yalnızca soyut alanını oluşturmakta ve veri olarak nitelendirilmek durumundadır.

sağlayan birleşik sunucular ağı ve bu ağdaki her bir sunucu, içeriğindeki veriler ile ayrılmaz bir bütün oluşturarak birer bilişim sistemi niteliğine sahip olurlar. Lakin verilerin oluşturduğu ve internet kullanıcılarının duyu organları vasıtasıyla anlamlandırabildiği bu dijital ortam/siber uzay, bilişim sistemi nitelemesi için gerekli olan ‘’donanım + veri/yazılım‘’ birleşimini sağlayamamaktadır. Bu sebeple de yalnızca verilerden oluşan soyut alanlar, bilişim sistemi olarak nitelendirilemez.

2.1.2.4. Sanallaştırma Uygulamaları ve Sanal Alanların Bilişim Sistemi Niteliği Sorunu

Bugün sahip olunan teknoloji sayesinde bilişim sistemlerinin verilerden oluşan soyut alanı bölünebilmekte, aynı şekilde ağ yapıları da mantıksal olarak bölünerek tek bir fiziksel bağlantı noktası bulunmasına rağmen, birbirinden bağımsız birden fazla sanal ağ yapısı yaratılabilmektedir. İşte tüm bu işlemler ‘’sanallaştırma‘’ olarak adlandırılır.[61] Örneğin bir LAN üzerindeki on fiziki sunucunun onu da kendi içinde on ayrı sanal birime bölünebilir, fiziki sunucular ve bunların sanal olarak bölünmüş yapılarına ayrı ayrı IP ve port taksimleri yapılarak çok sayıda ayrı müşteriye bulut sunucu hizmeti verilebilir. İstenirse LAN da on parçaya bölünerek on adet VLAN’da sunucular ayrı ayrı işletilebilir, sunucular üzerindeki işletim sistemleri de bölünerek her bir sanal alana birlikte çalışacak şekilde Linux ve Windows kurulabilir. Böylece on adet fiziki sunucu ve switch+router görevi gören tek bir modemden oluşan ağ yapısı, sanal olarak birbirinden bağımsız çok sayıda parçaya bölünmüş hale getirilebilir.

Bu tür yapılarda sanal makinelerin, sanal makinelerin bölünen işletim sistemlerinin ve fiziki makinelerin hangilerinin bilişim sistemi sayılması gerektiği ise tartışmaya değer bir konudur. Veriler üzerinde işlem gerçekleştiren fiziki makineler donanım ve verilerin birleşiminden oluştuğundan, sanallaştırılmış parçaların da özgül varlıkları kadar sunucuların fiziki alanını kaplayacağını ifade etmek mümkündür. Öyleyse örnekteki fiziki sunucular ve modemin bilişim sistemi olduğu açık olup, sunucuların sanallaştırılmış bölümlerinin de ayrıca bilişim sistemi sayılması doğru bir yorum olacaktır. Ağ yapıları da nihayetinde bilişim sistemlerinin birleşiminden

[61] Wikipedia, *Sanallaştırma*, tr.wikipedia.org/wiki/Sanalla%C5%9Ft%C4%B1rma_(bili%C5%9Fim), (ET: 02.03.2022); Wikipedia, *Network Virtualization*, en.wikipedia.org/wiki/Network_virtualization, (ET: 02.03.2022).

oluştuğundan, aynı yorumun ağların sanallaştırılmış birimleri açısından yapılması da mümkündür.

2.1.2.5. Bilişim Sistemi Kavramını Somutlaştırıcı Örnekleme

Bilişim sistemi kavramının eşlenik biçimde işleyen pek çok sistemin bağlı olduğu bir ağ yapısı ile örneklendirilmesi, konunun anlaşılmasına fayda sağlayacaktır. Bir bilişim sistemi olan Raspberry Pi kart, bağlantı portları ile diğer parçaların da bağlanmasıyla, ev içerisinde gezinen tekerlekli veya drone şeklinde uçan bir kamera haline getirilebilir. İşyerindeyken evin her noktasında olup bitenleri tek bir hareketli kamera ile izlemek isteyen kişi, elindeki bu IoT bilişim sistemini/kamerayı, wi-fi teknolojisi ile yine bir bilişim sistemi olan modem+routera bağlayarak, bir bütün olarak üçüncü bir bilişim sistemini teşkil edecek LAN ağını oluşturabilir. Bir diğer bilişim sistemi olan akıllı cep telefonuna ve IoT cihazına yüklediği yazılım vasıtasıyla, iş yerinde bulunan bu kişi ağ bağlantısı sayesinde IoT kamerasını yönetebilir ve kamera kaydını anlık izleyebilir. Bunun için IoT kamera ile akıllı cep telefonunun internet omurgası/WAN üzerinden ve erişim sağlayıcının omurgadaki bilişim sistemlerini kullanarak iletişim kurması gerekir. Erişim sağlayıcının omurga sistemleri, IoT kameranın dahil olduğu ev LAN'ı ve akıllı cep telefonunun hep birlikte oluşturdukları WAN da ayrıca bir bilişim sistemi olarak nitelendirilir.

2.1.3. Mevzuat, Yargı Kararları ve Doktrin Görüşleri Çerçevesinde Türk Hukukunun Bilişim Sistemi Kavramına Verdiği Anlam

2.1.3.1. Mevzuat

Yürürlükte bulunan pozitif hukuk metinlerinde, veriler üzerinde çeşitli işlemleri gerçekleştirme kabiliyetine sahip sistemler yönünden yeknesak bir isimlendirme yapılmamıştır. TCK'nın geneli ve sair bir kısım mevzuatta doğrudan ''bilişim sistemi'' sözcükleri kullanılmış, TCK md. 245/A ile 5271 s. Ceza Muhakemesi Kanunu[62] ve 5846 s. Fikir ve Sanat Eserleri Kanunu[63] başta olmak üzere diğer bir kısım mevzuatta ''bilgisayar'' sözcüğü üzerinden bir isimlendirmeye gidilmiş, aşağıda aktarıldığı üzere sair alanlardaki mevzuatlarda ise aynı işleve sahip sistemlere yönelik farklı isimlendirmeler yapılmıştır. Farklı isimler kullanılarak mevzuatta yer verilmiş bu teknolojik aletlerden/yapılardan hepsinin benzer işlevleri yerine getiriyor olması

[62] Yayımlandığı Resmî Gazete: Tarih: 17/12/2004 Sayı: 25673
[63] Yayımlandığı R.Gazete: Tarih: 13/12/1951 Sayı: 7981

sebebiyle eğer temel isimlendirme ‘’bilişim sistemi‘’ sözcükleri üzerinden yapılacak ise bunların tümünün bilişim sistemi kavramı içerisine giriyor olduğu aşikardır.

Mevzuatta geçen isimlendirme ve tanımlara, Anayasa md. 90 gereğince normlar hiyerarşisinin en üstünde bulunan ASS'nin ilk maddesinden başlamak gerekirse, ASS md. 1'de bilişim sistemleri tanımlanırken ‘’bilgisayar‘’ sözcüğü tercih edilmiş ve bu kavram ‘’*bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihaz*‘’ şeklinde tanımlanmıştır. Sözleşmenin hazırlanış sürecindeki teknolojik gelişmişlikte, toplumsal kullanımda bilgisayarlar haricinde pek fazla benzer cihaz bulunmamaktaydı. Lakin yıllar içinde durum değişmiş, bu sebeple Siber Suçlar Sözleşmesi Komitesi 2012'de gerçekleştirdiği 8. genel kurulunda, ASS'nin açıklanması için kılavuz notlar yayınlamaya karar vermiş ve bu notlarda sözleşmede yer alan ‘’bilgisayar‘’ kavramının akıllı telefonlar ve benzer sair bütün bilişim sistemlerini kapsayacak şekilde geniş manalı anlaşılması gerektiği, 2006 yılında konunun detaylı olarak tartışılarak bu sonuca varıldığı belirtilmiştir.[64] Ancak sözleşmenin lafzında direkt olarak bilgisayar sözcüğü kullanılması bazı karışıklıklara sebep olma potansiyeli taşımaktadır. Zira ASS'nin açıklayıcı raporunda ‘’sözleşmede bilişim sistemine eşdeğer olarak kullanılan bilgisayar sözcüğü değil‘’ bir bilişim sistemi olan ‘’bilgisayar‘’ açıklanırken, ‘’*bilgisayar farklı programları çalıştırabilir*‘’ denilmiştir.[65] Her ne kadar sözleşmede veya açıklayıcı raporunda bir teknolojik cihazın hukuken bilişim sistemi sayılabilmesi için mutlaka birden fazla programı çalıştırabilir veya ayrı ayrı işlevleri yerine getirebilir olması şart koşulmamış ise de bugün için en azından Türk hukuk doktrini ve uygulamasındaki bazı görüşler tarafından bu şartın koşulduğu görülmektedir.[66] Detaylı olarak incelendiğinde ise Türk hukukundaki bu yorumun ASS ve bağlantılı belgelerinde direkt olarak bir dayanağının olmadığı görülecektir. Kanaatimizce ASS'nin bilgisayar sözcüğü üzerinden tanımladığı bilişim sistemi kavramında aradığı temel işlev; verileri otomatik olarak işleyebilme yeteneği olup, sistemin birden fazla iş için kullanılabiliyor veya farklı uygulama yazılımlarını çalıştırabiliyor ya da genel amaçla kullanılabiliyor olması şartı aranmamıştır. Bu sebeple açıklayıcı raporda anlatılan bilgisayar cihazı ile sözleşme

[64] Cybercrime Convention Committee (2012), *T-CY Guide Note 1, On The Notion of ‘’Computer System‘’*,rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e6, (ET: 02.03.2022).
[65] ASS Açıklayıcı Raporu, https://rm.coe.int/16800cce5b, (ET: 02.03.2022).
[66] Bu yorumlar aşağıda aktarılmıştır.

metninde kullanılan ve bilişim sistemi kavramına karşılık gelen ‘’bilgisayar‘’ sisteminin birbiri ile karıştırılmaması, yorumlamaların da bu durum gözetilerek yapılması elzemdir.

Mevzuatımızda yer alan kanunlarda, bilişim sistemi veya aynı yeteneklere sahip cihazların tanımlandığı bir norm mevcut değildir. TCK md. 243'ün herhangi bir bağlayıcılığı bulunmayan gerekçesinde ise ‘’*Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma imkânı veren manyetik sistemlerdir*‘’ tanımlaması yer almaktadır. Mevzuatımızdaki yönetmeliklerde ise bilişim sistemi kavramının gerek direkt olarak gerekse farklı isimler ile çeşitli tanımlarına ulaşmak mümkündür. Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği md. 4/1-ğ'de kurumsal bilişim sistemi, ‘’*Kuruluş çalışanları tarafından kullanılan bilgisayarlar, bunlara hizmet veren dosya, uygulama, veri tabanı ve e-posta sunucusu ve ağ altyapısının tamamı*‘’ şeklinde tanımlanmıştır. Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik md. 3/1-b'de bilişim sistemi, ‘’*Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem*‘’ şeklinde tanımlanmıştır. Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ md. 3/1-a'da ise bilişim sistemleri, ‘’*Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, veri ve bunların sunumunda yer alan sistemleri*‘’ şeklinde[67] tanımlanmıştır. Ulusal Mobil Uyarı Sisteminin Kurulmasına ve İşletilmesine İlişkin Yönetmelik md. 3/1-b'de ise cihaz ‘’*Veri işleme ve saklama yeteneği bakımından, bilgisayarın özelliklerine benzer özelliklere sahip mobil telefonlar*‘’ şeklinde tanımlanmıştır. Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik md. 3/1-e'de bilgi sistemleri (BS),

[67] Benzer bir tanıma, Ulaştırma Bakanlığı'nın 2016-2019 Ulusal Siber Güvenlik Strateji ve Eylem Planı içerisinde de ulaşmak mümkündür. İlgili tanım ise ‘’*Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve bilgi/verinin sunumunda yer alan sistemler*‘’ şeklindedir. Ayrıca belgede geçen diğer ilişkili tanımlar şöyledir: Endüstriyel Kontrol Sistemleri: *Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan, SCADA (Supervisory Control and Data Acquisition) ve Dağınık Kontrol Sistemleri şeklinde gruplanan bilgi sistemleri /* Kamu bilişim sistemleri: *Türkiye Cumhuriyeti kamu kurum ve kuruluşlarına ait olan ve/ veya kamu kurum ve kuruluşları tarafından işletilen bilişim sistemleri /* Gerçek ve tüzel kişilere ait bilişim sistemleri: *Türkiye Cumhuriyeti kanunlarına tabi olarak gerçek ve tüzel kişilere ait olan ve/veya gerçek ve tüzel kişilerce işletilen bilişim sistemleri.*

''*Bilginin toplanması, işlenmesi, saklanması, dağıtımı ve kullanımına yönelik insan kaynağı, operasyonel faaliyetler ve süreçler ile bunlarla etkileşim içinde bulunan bilgi teknolojiler*''

şeklinde, md. 3/1-ğ'de ise bilgi teknolojileri (BT),

''*Herhangi bir biçimdeki verinin, girişinin yapılması, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim altyapısı ve ilgili diğer teknolojileri*''

şeklinde tanımlanmıştır. Bilgi sistemi olarak adlandırılan bir kavramın başka bir tanımı ise Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği md. 3/1-ç'de, ''*İşletim sistemlerinin, veritabanlarının, sunucuların, altyapının, iş uygulamalarının, kullanıma hazır ürünlerin, donanımların, yazılımların ve hizmetlerin tamamı*'' şeklinde yer almaktadır. Bilgisayarlar ve Bilgisayar Sunucuları ile İlgili Çevreye Duyarlı Tasarım Gereklerine Dair Tebliğ(*SGM-2015/4*) md. 4'te ise doğrudan bilgisayarın,

''*mantıksal işlemler gerçekleştiren, verileri işleyen, giriş aygıtlarını kullanma ve bilgi çıktılarını ekranda görüntüleme yeteneğine sahip ve normalde işlemler gerçekleştirmek üzere bir merkezi işlem birimi (CPU) içeren bir cihaz anlamına gelmektedir. CPU bulunmuyorsa cihaz, bilgisayarlı işlem birimi olarak çalışan bir bilgisayar sunucusuna istemci ağ geçidi işlevi görmektedir*.''

şeklinde bir açıklaması bulunmaktadır.

2.1.3.2. Yargı Kararları

Maddi ceza hukuku yönünden yüksek yargı kararlarında, bilişim sisteminin TCK md. 243'ün gerekçesinde yer alan tanımının benimsendiği görülmektedir.[68] Usul hukuku ve CMK uygulamasında da CMK md. 134 yönünden genel olarak md. 243'ün gerekçesindeki bu tanıma uyan bilişim sistemlerinin normun uygulama kapsamında

[68] ''*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.*'' Yargıtay CGK 2012/1293 E. 2013/111 K.; ''*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*.'' İstanbul Bölge Adliye Mahkemesi 21. CD 2016/226 E. 2016/247 K.

değerlendirildiği görülmektedir.[69] Yargıtay'ın maddi ceza hukuku yönünden spesifik olarak otomatların ve ankesörlü-kartlı telefonların bilişim sistemi olarak değerlendirilmesi gerektiğine dair kararları mevcut olduğu[70] gibi ATM'lerin bilişim sistemi sayıldığına[71] fakat kredi kartının bilişim sistemi olmadığına[72] yönelik kararları

[69] ''*CMK'nın 134 . maddesinde geçen bilgisayar teriminden ne anlaşılması gerektiği konusu CMK'da açık bir şekilde belirtilmemiştir. Bilgisayar; belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçları ifade etmektedir. Genel olarak 134. maddesinin uygulamada; bilgisayar, akıllı telefonlar, GPS cihazları, donanım ve yan donanımlar, verileri dijital olarak kaydetme ve işleme yeteneğinde olan her türlü dijital cihazları kapsadığı kabul edilmektedir. Aynı şekilde madde kapsamına; içağlar, veri tabanları, sistem odaları, sunucular, yedek üniteler, arşivler, veri iletim hatları, yönlendiriciler vs. dâhilinde bulunan tüm dijital alanlar, veriler ve veri taşıyıcıları da girmektedir. Zira bunlar belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçlar olan bilgisayarların bileşenleri olarak fonksiyon icra etmektedir.*'' Yargıtay CGK 2016/544 E. 2020/127 K.

[70] ''*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 barkod numaraları, görüşen ve görüşülen bölgeler ve numaralar, görüşme saati ve süresi v.s) bünyesinde topladığı anlaşılmaktadır. Nitekim kopyalama yapılan manyetik kartların barkod 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. ... 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 CGK 2007/136 E. 2007/150 K.; ''*... T. T. A.Ş. tarafından üretilen ve ankesörlü telefonlardan konuşma yapmaya yarayan telefon kartlarının manyetik şeritlerine teyp bandı ile dolum yapmak suretiyle kaçak görüşme yaptığının iddia ve kabul olunması karşısında; gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin bulunmaması nedeniyle dolandırıcılık suçunun unsurlarının bulunmadığı, ayrıntıları Ceza Genel Kurulu'nun 19.06.2007 gün ve 136-150 sayılı kararında belirtildiği üzere sanığın fiilinin kül halinde suç tarihinde yürürlükte bulunan 765 sayılı TCK.nun 525/b-2 (5237 sayılı TCK.nun 244/4 maddesine uygun "bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama") madde ve fıkrası kapsamında bilişim suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde karar verilmesi ...*'' Yargıtay 11. CD 2006/1800 E. 2008/7126 K.

[71] Yargıtay CGK 2007/136 E. 2007/150 K.

[72] Yargıtay 8. CD: 2014/30107 E. 2015/1395 K.

da bulunmaktadır. Akıllı telefonların da Yargıtay uygulamasında bilişim sistemi olarak nitelendirildiği görülmektedir.[73]

TCK md. 243'ün gerekçesinde yer alan ''*Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma imkânı veren manyetik sistemlerdir*'' şeklindeki tanımlamada hukuken bilişim sistemi sayılabilecek cihazların ''genel kullanıma uygun ve bir çok işlevi yerine getirebilir olması'' şartı bulunmamaktadır. Ayrıca yukarıda detaylı olarak açıklandığı üzere ASS'deki tanımlama ve sözleşmeye dair resmi açıklamalardan da böyle bir anlam çıkarılamamaktadır. Lakin Yargıtay'ın maddi ceza hukukuna dair pek çok kararında, bir teknolojinin bilişim sistemi sayılabilmesi için bu sistemin olmazsa olmaz özelliğinin ''genel amaçlı kullanım'' olduğu zikredilmektedir. İlgili görüşe göre bir teknolojik cihazın, üretim şekli gereğince yalnızca belirli bir fonksiyonu yerine getirebilen ve başka bir fonksiyon ifa edemeyen bir yapıda bulunması, hukuken bilişim sistemi olarak nitelendirilmesinin önüne geçecektir.[74]

---

[73] ''*Bilgisayarın çalışmasını düzenleyen tüm programlara işletim sistemi denilmekte olup işletim sistemlerinin sadece bilgisayarlarda değil cep telefonlarında, tablet PC'Ierde 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. En çok kullanılan ve en çok bilinen işletim sistemleri aşağıda örneklendirilmiştir. · Unix - Unix Çeşitleri / System V, BSD, Solaris, AIX.. / · Linux - Linux Dağıtımları / Pardus, Ubuntu, Fedora, Debian.. / · Windows - Windows Sürümleri / Windows 7, Windows 8, Windows Server 2012 / · MacOS - MacOS/IOS Sürümleri / OS X, IOS / · Android Windows: Microsoft şirketinin geliştirdiği Windows (pencereler) kullanıcıya grafiklerle ve görsel iletilerle yaklaşarak, yazılımları çalıştırmak, komut vermek gibi klavyeden yazma zorunluluğunu ortadan kaldıran, dünyada en çok kullanılan işletim sistemidir. En çok kullanılan sürümü Windows 7 olup özellikle tablet PC'Ier için Windows 8 geliştirilmiştir. Apple İOS: İOS eski adıyla (IPhone OS) Apple'ın orjinal olarak iPhone için geliştirdiği ancak daha sonra iPod Touch ve İPad'de kullanılan mobil işletim sistemidir. Android: Cep telefonlarında ve tabletlerde en çok kullanılan mobil işletim sistemi olan Android'in en yaygın sürümleri 2.3 Gingerbread, 4.0 Ice Cream Sandvvich , 4.1 Jelly Bean'dır. ... 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 …*'' Yargıtay 8. CD 2014/30037 E. 2015/14023 K.

[74] Yargıtay 8. CD 2018/1810 E. 2019/6992 K.; ''*Bu tanımlamalardan da anlaşıldığı üzere, bilişim sistemi, bilgisayara göre daha geniş bir alanı kapsayan bir üst kavramdır. Bilişim sisteminde veri iletişimi, bilgisayarla birlikte, elektronik, manyetik veya bazı mekanik araçlarla bir ağ üzerinden sağlanabilir. Bilişim suçları ise, verilere ve/veya veri işlemle bağlantısı olan sistemlere karşı bilişim sistemleri aracılığıyla işlenen suçlar olarak tanımlanabilir. ... Bilişim suçlarının çok geniş ve sürekli ilerleyen bir alan olması nedeniyle 5237 sayılı TCK. nunda öğretide görüş birliğiyle bilgisayara karşılık geldiği belirtilen "bilgileri otomatik işleme tabi tutan sistem" yerine bu tür araçlarla işlenen suçları da kapsayabilmesi ve yeni teknolojik ilerlemelere açık olması amacıyla "bilişim sistemi" terimi kullanılmıştır. İster "bilişim sistemi" isterse "bilgileri otomatik işleme tabi tutmuş" sistem kavramı kullanılsın bununla ifade edilmek istenen genel amaçlı kullanıma müsait bilgisayarlardır. Yoksa tek*

2.1.3.3. Doktrin Görüşleri

Ceza hukuku yönünden hangi teknolojik yapıların ve cihazların bilişim sistemi olarak kabul edileceğine dair doktrinde çeşitli görüşler mevcuttur. Bu görüşler teknolojinin işleyişinin sunduğu işlem kapasitesinin gelişmişliğine bağlı olarak belirli şartlar koşmakta ve bazı hukuki görüşlere göre sınırlı işlemleri yerine getiren teknolojiler de bilişim sistemi sayılabilecekken, sair bazı görüşler bilişim sistemi sıfatının kazanılması için veriler üzerinde gerçekleştirilen bu işlemlere başkalarının da eklenmesi gerektiğini şart koşmaktadır.

Doktrinde bazı yazarlar, hukuki manasıyla bilişim sistemi kavramının; otomatik olarak verileri toplama, depolama, aktarma, çoğaltma, düzenleme, değerlendirme ve sair işlemler ile bağlantılı bir kavram olduğunu belirtmektedir. Lakin bu açıklamalardan bilişim sistemi sıfatının bu işlemlerden asgari olarak hangilerini gerçekleştirebilen cihazlarda olması gerektiği yönünde spesifik bir yoruma ulaşılamamaktadır.[75]

Doktrinde en genişletici yorum, verileri otomatik olarak işleyebilen her türlü sistemin hukuken de bilişim sistemi olarak kabul edileceği görüşüdür.[76] Diğer bir

---

amaçlı çalışan bilgisayar destekli veya bilgisayar özelliklerinin bir kısmına haiz aletler ile atanmış bilgisayarlar bu yasanın kastettiği bilişim sistemi tabiri içinde değerlendirilemezler. …. Bilişim özeliliğine sahip bilgisayarı diğer aygıtlardan ayıran özellik de budur: Genel kullanabilme özelliğine sahip bir araç olmasıdır. Diğer bir ifade ile bilgisayarın dışında veya bilgisayar destekli yahut bilgisayar benzeri araçlar da bilginin otomatik işlenmesine yönelik olarak çalışabilir, ancak bunlar ile bir veya birkaç amaçlı işlem yapılabilir yoksa bilgisayar gibi bilişim alanının tamamını kapsayıcı nitelikte işlemler değil, yani atanmış bilgisayarlar bilişim özelliğine sahip araç değildirler: Örneğin, elektronik hesap, makineleri, TV. ler, çamaşır makineleri, diyaliz makineleri, röntgen cihazları, decoderler, hatta dalış bilgisayarları, arabaların yol bilgisayarları vs. bilişim alanında alanın temelini bilgisayarlar oluşturmaktadır. … Bir faaliyetin bilişim faaliyeti olup olmadığını tarif edebilmek için, o faaliyetin bilgisayar sistemine dahil olup olmadığına bakmak gerekir. Daha açık bir ifadeyle şu sorunun cevabı verilmek gerekir. Faaliyet bilgisayar sistemiyle mi temellenmektedir; yoksa bilgisayar o faaliyetin gerçekleşmesine yardımcı bir unsur olarak mı kullanılmaktadır? Yani bilgisayar desteklimidir? Bankaların ATM uygulaması bilgisayar destekli olduğu için bilişim faaliyetidir. Zira bu sistem herhangi bir nedenle çöktüğünde bu faaliyet de asla gerçekleşmez. Bunun karşıtı bir örnek verilecek olursa, uçak firmalarının bilet satışlarında bilgisayar sistemlerinden yararlanmaları yani faaliyetin bilgisayar destekli olması bir bilişim faaliyeti değildir. Çünkü bu sistemler bu firmaların faaliyetini kolaylaştırmakla hızlandırmakla ve daha verimli kılmakla birlikte faaliyetin tarif edici unsuru değildir. '' Yargıtay CGK 2007/6-13 E. 2007/150 K

[75] Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1150; Hatice AKINCI, A. Emre ALIÇ, Cüneyd ER (2004), ''Türk Ceza Kanunu ve Bilişim Suçları'', İçinde, *İnternet ve Hukuk,* Derleyen: Yeşim M. Atamer, ss.157-277, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, s. 170; Mesut ORTA (2015), *Bilişim Suçlarında Adli Analiz*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Konya, s. 23; Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 957; Fazıl GÜRLER (2013), *Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar,* Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara, s. 11; Hasan Burak ÖNDİN (2017), *Türk Hukukunda Doğrudan Bilişim Suçları*, Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Eskişehir, s. 4, 5.

[76] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 236.

görüşe göre ise bilişim sisteminin verileri işleyebilmesi ve depolayabilmesi şart olup, aktarım sağlayabilmesi bilişim sistemi sıfatına sahip olması için şart değildir.[77] Belirtmek gerekir ki verileri otomatik olarak işleyebilen bir cihaz, işlenecek asgari bir veri bütününü kendi içerisinde barındırmıyorsa, tek başına bu işlemi gerçekleştiremez. Bu sebeple ilk görüşün de temelde bu gömülü verileri es geçmediği varsayılabilir. Öyleyse hukuken bilişim sisteminin sahip olması gereken işlem kabiliyetlerine dair en genişletici yorum, otomatik olarak verileri depolamak ve işlemek şeklinde anlaşılmalıdır.

Teknik olarak bilişim sistemleri temelde verileri otomatik olarak işler ve bunu yapabilmek için de asgari yazılımları gömülü olarak donanımlarında barındırır. Bu veri işleme-depolama işlemlerine ek olarak veri aktarma kabiliyeti sağlanması için sistemin yazılımlarının buna elvermesi ve ayrıca ağ bağlantı çıkışlarının, örneğin USB portunun bulunması gerekir. Öyleyse veri aktarma işlemini teknik anlamda verileri işleyip depolayan her sistemin gerçekleştiremeyebileceği belirtilmelidir.

Veriler üzerinde daha fazla işlemi yerine getirebilir olmayı şart koşan görüşlerden kısmen genişletici bir yoruma göre ise bilişim; verilerin işlenmesi ve aynı zamanda aktarılmasını konu etmekte olup, bu yöndeki teknolojilere bilişim sistemi denilmektedir. Ancak bu görüşe sahip olan yazarlardan Akbulut, bilişim sistemlerini donanım ve yazılımların birlikte işleyişi olarak nitelendirdiğinden, Akbulut ve bu yöndeki sair görüşlerin bir önceki paragrafta olduğu gibi zımnen verilerin depolanmasını da bu işlemler arasında saydığı varsayılmalıdır. Öyleyse ilgili görüşlere göre hukuken bilişim sistemi sıfatı için verileri işleme ve depolamanın yanında aktarma özelliğinin bulunması da gerekmektedir.[78]

Hukuken bilişim sistemi sıfatının varlığı için gerçekleştirilebilen işlem kabiliyetlerinin daha da fazla olması gerektiği yönündeki görüşlerden ilki ise ‘’*bilgiyi dijital olarak işleyebilen, depolayabilen, üretebilen ve aktarabilen aygıtlar*‘’ şeklindeki tanımlama ile oluşan görüştür.[79] Bu noktada ‘’*Bilişim sistemi, verilerin saklanmasını, toplanmasını, işlenmesini, değerlendirilmesini, depolanmasını ve*

[77] ‘’*Bilişim sistemi; manyetik, optik veya elektriksel ortamlarda bulunan veriyi sayısal olarak işleyebilen, saklayabilen ve/veya iletebilen cihaz veya cihazlar bütününe verilen* isimdir.‘’ Hamza Aytaç DOĞANAY (2020), *Mobil Cihaz Adli Bilişiminde Karşılaşılan Güncel Zorluklar ve Delil Zinciri*, Legem, Ankara, s. 8.

[78] Berrin AKBULUT 2017, age. s. 124; Ali İhsan ERDAĞ (2010), ‘’Bilişim Alanında Suçlar(Türk ve Alman Ceza Hukukunda)‘’, *Gazi Üniversitesi Hukuk Fakültesi Dergisi* C. 14, S. 2, ss. 275-303, s. 277, 278.

[79] Murat Volkan DÜLGER 2022, age. s. 67, 68, 69 vd.

aktarılmasını sağlayan sistemdir'' şeklindeki tanımlama ile oluşan sair bir görüşü de aktarmak gerekir.[80] Bu görüşlerde yukarıdakilere ek olarak, ''verileri üretme'' kabiliyetinin de sayıldığı görülmektedir. İkinci görüşte veriyi üretme yeteneğine ek olarak, ''verileri değerlendirme'' kabiliyeti de sayılmıştır.

Veriler üzerinde yukarıda sayılanlardan daha fazla işlemi yerine getirebilir olmayı şart koşan ve en daraltıcı görüş ise

> ''*verileri toplayabilme, saklayabilme, işleyebilme, çoğaltabilme, değerlendirebilme ve aktarabilme özelliklerine sahip olan ve bu fonksiyonları çok yönlü olarak otomatik işlemlere tabi tutma*''

işlemlerinden hepsini gerçekleştirebilen sistemlerin hukuken bilişim sistemi sıfatına sahip olabileceği yönündeki görüştür. Bu görüşe göre sistemin birden çok fonksiyonu yerine getirebilir olması da ayrıca şarttır ve örneğin veriler üzerinde tüm bu sayılan işlemleri gerçekleştirebilse dahi tek fonksiyonlu olan teknolojik cihazlar bilişim sistemi sayılamazlar.[81] Bu yorum, Yargıtay kararları aktarılırken belirtildiği üzere bazı kararlarda şart koşulan ''*genel kapsamlı-genel amaçlı kullanıma uygun olma*'' hususu ile çok benzerdir. Doktrinde hukuken bilişim sistemi sayılacak teknolojilerin genel amaçlı kullanıma uygun/genel kapsamlı olarak çalışmasının şart olduğunu belirten sair görüşler de mevcuttur.[82] Aynı yöndeki bir diğer görüşe göre ise otomatlar, aynı gerekçe sebebiyle ve farklı program yüklenememelerinden ötürü bilişim sistemi sayılamazlar.[83]

İşlem kabiliyetlerine göre koşulan bu şartların dışında, verilerin hangi ortamlarda barındırıldığı zaman sistemin hukuken bilişim sistemi sayılması gerektiğine dair de doktrinde çeşitli görüşler mevcuttur. Bu görüşlerin dile getiriliyor oluşunun sebebi, TCK md. 243'ün gerekçesinde bilişim sistemleri için ''*manyetik sistemler*'' tabirinin kullanılmış olmasıdır. Doktrinde bilişim sistemlerinde verilerin manyetik, optik ya da elektriksel ortamlarda bulunabileceği[84] yönünde görüşler mevcut olduğu gibi TCK md. 243'ün gerekçesini baz alarak manyetik olmayan sistemlere hukuken bilişim sistemi denilmesinin imkansızlaştığı yönünde görüşler de

---

[80] *Dijital Ceza Muhakemesi Hukuku*, Ed. Bahri ÖZTÜRK, Durmuş TEZCAN ve Mustafa Ruhan ERDEM (2021), Seçkin, Ankara, s. 32.
[81] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. 898, 899.
[82] Muammer KETİZMEN (2006), *Türk Ceza Hukuku'nda Bilişim Suçları*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Ankara, s. 19; Cengiz APAYDIN (2017), *Bilişim Suçları ve Bilişim Ceza Hukuku*, İstanbul, s. 39.
[83] Fazıl GÜRLER 2013, age. s. 102
[84] Hamza Aytaç DOĞANAY 2020, age. s. 8.

mevcuttur.[85] Ancak bu görüşün sahibinin de yazarı olduğu sair bir eserde dile getirilen bir yorumda, gerekçenin yanlışlığı ve manyetik olmayan sistemlerin de bilişim sistemi olabileceği zikredilmektedir.[86]

Hukuken bilişim sistemi olarak nitelendirilebilecek teknolojik yapıların genel niteliklerine dair görüşler aktarıldıktan sonra, spesifik olarak hangi cihazların veya cihaz birleşimlerinin ya da cihazlar arası ağ yapılarının hukuken bilişim sistemi sıfatını kazandıklarına dair bir kısım görüşleri aktarmak gerekmektedir. Evvela belirtmek gerekir ki doktrindeki hakim görüş, Türk pozitif hukuku ve TCK'nın bilişim sistemi kavramından kastının yalnızca tablet, masaüstü, dizüstü ve sair ''bilgisayar'' cihazları olmadığıdır. Hakim görüşe göre bu kavram, bilgisayar cihazlarını çatısı altına alan lakin bundan çok daha büyük bir kavramdır.[87] Bu sebeple TCK'nın genelinde,[88] CMK ve FSEK gibi sair mevzuatın aksine bilgisayar değil bilişim sistemi kavramının kullanılması olumlu karşılanmaktadır.[89]

Bilişim sistemi sayılacak teknolojilere dair spesifik nitelendirmelere göre araç bilgisayarlarını[90] ve GSM ya da CMDA ağları üzerinden elektronik haberleşme yapabilmesi haricinde benzer yapıda bulunan akıllı cep telefonlarını[91] bilişim sistemi olarak nitelendiren görüşler mevcuttur. Yine veriler üzerinde çeşitli işlemleri gerçekleştirme kabiliyetine sahip oyun konsollarını da bilişim sistemi olarak

[85] İlker TEPE (2009), *Modern Ceza Hukuku Anlayışında İnternet Suçluluğu ve Türk Ceza Hukukundaki Yansımaları*, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Antalya, s. 271.
[86] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 958.
[87] Berrin AKBULUT 2017, age. s. 110; Hatice AKINCI, A. Emre ALIÇ, Cüneyd ER 2004, age. s. 172; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1150; Abdulrahman Hussein KAREEM (2019), *Bilişim Suçları*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Konya, s. 4; İbrahim ŞAHBAZ (2020), *Açıklamalı ve İçtihatlı Türk Ceza Kanunu Cilt 3*, Yetkin, Ankara, s. 3123; Ahmet Caner YENİDÜNYA (2005), ''Bilişim Sistemine Hukuka Aykırı Erişim Suçu'', *Legal Fikri ve Sınai Haklar Dergisi*, S. 4, s. 2, 7; Ali İhsan ERDAĞ 2010, age. s. 278, 279; Burak Cesur AKÖZ 2018, age. s. 13.
[88] TCK md. 245/A'da bilgisayar kavramı kullanılmıştır.
[89] ''*Yasada bölüm başlığı olarak "bilişim alanında suçlar" ibaresinin kullanılması yerinde olduğu gibi, madde içeriklerinde "bilgisayar" ya da "bilgileri otomatik işleme tabi tutan sistem" yerine, "bilişim sistemi" denilmesi de oldukça isabetlidir*.'', Ahmet Caner YENİDÜNYA 2005, age. s. 2.
[90] Burak Cesur AKÖZ 2018, age. s. 14.
[91] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 236; Hamza Aytaç DOĞANAY 2020, age. s. 16; Elif GÖKŞEN (2014), *Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri*, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul, s. 17, 18, 29 vd.

değerlendiren görüşler mevcuttur.[92] Sim kart,[93] USB, CD, hafıza kartı, hard disk[94] gibi otomatik olarak veri işleme, depolama, aktarma yeteneğine sahip harici ve/veya dahili veri depolama üniteleri de bilişim sistemi olarak kabul edilmektedir. Bunlara ek olarak bu tür donanımlara ve işlem kabiliyetlerine sahip kamera, fotoğraf makinesi ya da müzik çalar gibi cihazları bilişim sistemi kavramına dahil eden görüşler de mevcuttur.[95]

Doktrinde akıllı cihazları bilişim sistemi olarak nitelendiren görüşler[96] mevcut olduğu gibi bu cihazlardaki veri depolama ve işleme yeteneğini sağlayan gömülü sistemleri bilişim sistemi olarak nitelendiren görüşler de mevcuttur.[97] Doktrinde IoT kavramı kullanılarak açıklanan teknolojilerin de bilişim sistemi sayılacakları yönünde görüşler mevcut olmakla birlikte, IoT bir iletişim ağı teknolojisini temsil ettiği için bu noktada ilgili görüşlerde kast edilenlerin salt ağ yapılarına bağlı cihazlar değil, ağ yapıları ile birlikte esas olarak, veriler üzerinde otomatik olarak çeşitli işlemler gerçekleştiren tekil akıllı cihazların da kast edildiğini söylemek daha doğru olacaktır.[98] Doktrinde internet gibi iletişim ağlarını ve bu ağ teknolojilerinde yer alan sistemleri bilişim sistemi kavramının içerisinde değerlendiren görüşler de mevcuttur.[99]

2.1.3.4. Değerlendirme

Bölümün önceki alt başlıklarında, veriler üzerinde otomatik olarak çeşitli işlemleri gerçekleştirme kabiliyetine sahip teknolojik yapıların/cihazların/sistemlerin özellikleri ve gelişmişlik yapılarına göre sübjektif biçimde sıralamaları yapılmıştı. TCK ve/veya sair pozitif hukuk mevzuatını değil, teknik hususları baz alınarak yapılan açıklamalardan ortaya çıkan sonuç; akıllı cihaz, bilgisayarlı cihaz, bilgisayar, bilişim

---

[92] Murat ÖZBEK (2013), *Adli Bilişimde Delillerin Toplanması ve İncelenmesi,* İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Yüksek Lisans Programı Yüksek Lisans Tezi, İstanbul, s. 27. Yazar ilgili değerlendirmeyi CMK md. 134 ve adli bilişim nazarında yapmıştır. Ancak bilişim sistemi teknik bir yapı olduğundan, bu yapı hukukun her alanında aynı olguyu ifade edecektir.
[93] Hamza Aytaç DOĞANAY 2020, age. s. 76.
[94] Age. s. 8; Berrin AKBULUT 2017, age. s. 126.
[95] Elif GÖKŞEN 2014, age. s. 17, 18, 19, 20, 21 vd.
[96] Emre İkbal AÇIKGÖZ (2017), *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu*, Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara, s. 8, 9.
[97] Mesut ORTA 2015, age. s. 24.
[98] Berrin AKBULUT 2017, age. s. 126; Emre İkbal AÇIKGÖZ 2017, age. s. 9; Büşra ÖZÇELİK (2019), *Bilişim Sistemine Girme Suçu,* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul, s. 11.
[99] Berrin AKBULUT 2017, age. s. 125; Emre İkbal AÇIKGÖZ 2017, age. s. 10, 11, 12; İlker TEPE 2009, age. s. 271; Elif GÖKŞEN 2014, age. s. 17, 18, 19, 20, 21 vd.; Cengiz TANRIKULU (2014), *Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, s. 11; Mesut ORTA 2015, age. s. 24.

cihazı, bilişim sistemi, bilgi iletişim teknolojisi ve sair ne şekilde isimlendirilirse isimlendirilsin, bu teknolojilerin temel özelliğinin verileri otomatik olarak işlemesi ve bu işleme yeteneği için belirli yazılımları barındırmak zorunda olduğu için aynı zamanda verileri depolayabilme özelliğine de sahip olması gereğidir. Öyleyse asgari olarak verileri işleme **ve** depolama özelliğine sahip olan bu sistemlerin, maddi ceza hukuku ve hukukun sair alanlarında hukuken de bilişim sistemi sayılmaları gerekmektedir. Zaten ne ASS'de[100] ne TCK'da ne de sair bir mevzuatta verilerin ''işlenmesi'' dışında bir şart bu tür sistemler için yapılan tanımlamalarda geçmemektedir. Sınırları açıkça kanuni olarak çizilmemiş bir yapı yönünden kanunilik ilkesinin tecellisi de ancak bu yapının maddi gerçekler ile uyumlu, olduğu gibi kabul edilmesi ve sübjektif yorumların yapılmaması sonucu mümkün olabilir.

İlk paragrafta açıklanan sebepler dolayısıyla, doktrinde bir teknolojik yapının hukuken bilişim sistemi sayılması için verileri otomatik olarak işleme ve depolama yeteneğinin yanında farklı işlem yeteneklerine de sahip olmasını şart koşan görüşleri doğru bulmuyoruz. İkinci olarak, bu şartın yanında sistemlerin ancak genel amaçlı kullanılabilir olması durumunda hukuken bilişim sistemi sayılabileceklerine yönelik doktrin görüşleri ve yargı kararlarını da doğru bulmuyoruz.

Bu görüşlere katılmıyor olmamızın, ilk paragrafta zikredilenlerden farklı sebepleri de mevcuttur. Örneğin veri işleme ve dolayısıyla depolama özelliğine sahip herhangi bir bilişim sisteminin verileri değerlendirebiliyor olması için buna yönelik analiz kabiliyeti içeren yazılımları bünyesinde barındırması gerekir. Aynı şekilde verileri toplayabilme-aktarabilme yeteneği için bu sistemin hem yazılımında buna yönelik bir kabiliyet hem de donanımlarında veri aktarımına yönelik bağlantı portları, CD-kart okuyucuları ve/veya kablolu/kablosuz bağlantı kartlarının ya da sensörlerinin mevcudiyeti gerekir. Aynı şekilde ağ bağlantısı yapabilmek için de buna yönelik yazılım ve donanımların mevcudiyeti şarttır. Bu örneklerin çoğaltılması mümkündür ancak burada önemli olan husus; herhangi bir bilişim sisteminin ve en basit olarak Arduino ve sair mikro denetleyici kartların, üzerinde basit işlemler yapılarak yazılım ve donanımlarının geliştirilebilir yahut köreltilebilir olduğudur. En temel yeteneklere indirgenmiş ve salt işlemci çip ile sistemin çalışmasına dair gömülü verileri barındıran

[100] ASS'de bilişim sistemi kavramı ve spesifik bir cihaz olan bilgisayar kavramına verilen anlamlar ile neden çok fonksiyonlu bilgisayarlar ile sair bilişim sistemlerinin ASS özelindeki tanımlardan kaynaklı olarak birbirine karıştırılmaması gerektiğine yönelik açıklamalar için işbu tezin 31 ve 32. sayfalarına bakılmalıdır.

çipin bulunduğu bir kart, rastgele bir akıllı cihaz üzerinde sadece veri işleme ve depolamayı sağlayacak şekilde çalıştırılabilir. Aynı kartın üzerine bağlantı portları ve gerekli yazılımlar yüklendiği zaman, bu kart aynı zamanda ağ bağlantısı ve iletişimi sağlayacak şekilde IoT cihazlar üzerinde de konumlandırılabilir. Başka bir örnekte ise Raspberry Pi ile akıllı hale getirilmiş buzdolaplarında çok basit ek işlemler gerçekleştirilerek, bu sistemlerde bilgisayar/X-Box oyunları dahi oynanabilir veya fotoğraf çekilerek Instagram'a yüklenebilir ki bu tür ürünler halihazırla üretilmekte ve evlerde kullanılmaktadır.[101] Tersinden bir örnek vermek gerekirse, bir masaüstü bilgisayar üzerindeki bağlantı portları ve kartlar işlevsiz kılınarak, işletim sistemi sınırlandırılarak ve salt sistem ile grafik işlemci setleri kullanılabilecek hale getirilerek, bu bilgisayar sadece içeriğindeki mevcut veriler üzerinden sınırlı işlemleri yapabilecek hale getirilebilir.

Sistemler basit yapılandırmalar ile çok farklı niteliklere sahip olabileceği veya çok amaçlı bir kullanım olanağından yoksun bırakılabileceği için özünde verileri işleme ve depolama kabiliyetine sahip sistemler arasında ayrıma gidilmesinin normatif bir dayanağı olmadığı gibi bu ayrım son derece sakıncalı sonuçlar da doğurabilir. Örneğin çok amaçlı kullanıma uygun bir cep telefonu üzerinden SD ya da sim kartın içerisindeki verilere erişildiğinde farklı, tek amaçlı kullanılan dekoderler üzerinden içerisindeki SD ya da sim kartın verilerine erişildiğine farklı nitelendirmeler yapılmaması gerekir. Aynı şekilde, yalnızca video kaydında kullanılan IP kamera sistemlerinin, kameranın bağlı olduğu LAN'daki diğer bilişim sistemleri ile arasındaki trafiğin izinsiz olarak izlenmesi durumunda da kamera ve ağdaki sair sistemler arasında bilişim sistemi niteliğine dayalı bir ayrım yapılmamalıdır.

Nihai olarak şu hususu da vurgulamak gerekir ki bir bilgisayarın soğutucusunun, bir otonom arabanın sileceğinin veya bir akıllı buzdolabının raflarının bilişim sistemi kavramı ile hiçbir bağlantısı bulunmamaktadır. Bu sebeple bilişim sistemleri ile aynı yapısal bütünlük içerisinde bulunsalar dahi verilerin otomatik olarak işlenmesi, depolanması, aktarımı ve sair işlemler ile bir bağı olmayan parçaların bilişim sistemi kavramına dahil edilmesi mümkün değildir. Öyleyse bilişim sistemi sayılan yapı, soğutucu fanlarının da dahil olduğu bir bilgisayar kasası değil, temelde

[101] Bkz. Raspberry Pi, Wikipedia, https://tr.wikipedia.org/wiki/Raspberry_Pi, (ET: 20.06.2022) / Örnek bir buzdolabı için bkz. https://www.samsung.com/us/explore/family-hub-refrigerator/overview/, (ET:20.06.2022).

veriler üzerinde işlem gerçekleştiren donanımlar **ve** verilerin birlikte oluşturduğu yapı olmalıdır.

2.2. SİBER SALDIRILAR ve HACKİNG

2.2.1. Siber Saldırı Kavramı

Hukuk literatüründe, bilişim sistemleri ile ilişkili suç tiplerine yönelik ‘’bilişim suçu‘’ kavramı yerleşiktir.[102] Bilişim suçları, bilişim sistemlerinin yalnızca araç olarak kullanıldıkları geniş manada bilişim suçları ve suçun konusu ya da korunması amaçlanan değerinin bilişim sistemleri ile bağlantılı olduğu dar manada bilişim suçları şeklinde ikiye ayrılabilmektedir.[103] Dar manadaki bilişim suçlarının ve örneğin tez konusu olan TCK md. 243’te yer alan suçların tipikliği içinde kalan fiiller ise gerek hukuk doktrini gerekse hukuk dışı sosyal bilimler alanındaki doktrinlerde ‘’siber saldırılar‘’ olarak adlandırılır. Bilişim ve ağ teknolojileri ile siber güvenliğe dair spesifik kaynaklarda ise bu tür faaliyetlere en geniş boyutuyla, bir çatı kavram olarak ‘’hacking faaliyetleri‘’ denilmektedir.

Ulaştırma Bakanlığı 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı’nda siber saldırı, siber olay ve siber risk kavramları ayrı ayrı tanımlanmıştır. İlgili belgede siber saldırı

> ‘’*siber uzaydaki bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler*‘’

şeklinde, siber olay ‘’*bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğinin ihlal edilmesi*‘’ şeklinde[104] ve siber risk ise

---

[102] Murat Volkan DÜLGER 2022, age. s. 72, 73, 74, 75.

[103] Zeki AVŞAR ve Gürsel ÖNGÖREN (2010), *Bilişim Hukuku*, Türkiye Bankalar Birliği, İstanbul, s. 126. / Ali KARAGÜLMEZ 2014, age. s. 54, 55, 56, 57 / Dülger yalnızca dar manadaki bilişim suçlarının esas bilişim suçları olarak algılanması gerektiğini düşünmektedir. Bu konuda bkz. Murat Volkan DÜLGER 2022, age. s. 78, 79 / Şahıslara yönelik yapılan siber saldırılar, internet aracılığıyla hakaret suçunda olduğu gibi kişilik haklarını ihlal ettiğinde, bunlara siber zorbalık da denilebilmektedir. Bu konuda bkz. Servet YETİM (2015), ‘’Siber Zorbalık-Türkiye ve ABD Karşılaştırması(ABD V. DREW DOSYASİ)‘’, *TBB Dergisi*, S. 120, ss. 325-385, s. 328.

[104] Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ md. 3/1-e’de ise aynı kavram, ‘’*Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulması*‘’ şeklinde tanımlanmıştır.

''*siber tehditlerin bir veya birden çok bilgi varlığındaki açıklığı kullanarak zarar yaratma potansiyeli. Siber olayın olumsuz sonuçlarına ilişkin olasılıklar kombinasyonu*''

şeklinde tanımlanmaktadır.[105] Siber saldırılar ile siber olaylar arasında bir sebep-netice ilişkisi bulunur. Siber saldırılar neticesinde meydana gelen durum yani örneğin sistemin bozulması, siber olay olarak değerlendirilir.[106]

Siber saldırıların bilişim suçlarına yönelik bir boyutu olduğu gibi devletler arası genel hukuk/savaş-çatışma hukuku bağlamında ele alınan ve genel olarak Talinn Kılavuzu'nda detaylandırılan bir boyutu daha bulunmaktadır. Bu noktada artık bilişim suçları değil, devletler arası veya devletlere yönelik yapılan ve bilişim teknolojilerinin ''silah'' olarak kullanıldığı eylemler meydana gelir.[107] Siber saldırıları bilişim suçları ve savaş/çatışma hukuku bakımından her zaman net bir şekilde ayırmak mümkün olamamaktadır. Örneğin suç örgütü şeklindeki bir hacker grubunun devletlere karşı can veya ciddi mal kayıplarına sebep olacak siber saldırılarda bulunması, ceza hukukunun yanında savaş/çatışma hukukunun konusunu da oluşturabilir. Yine bu doğrultuda, başka bir devletin egemenlik alanı içerisindeki bu tür grupların diğer devletlere karşı siber saldırılarda bulunması ve grubun içerisinde barındığı egemen devletin saldırıları engellememesi durumunda da bu saldırılar yıkıcılık etkisine göre çatışma/savaş hukukunun konusunu oluşturabilecektir.[108]

İnternetin toplumsal bir kullanım olanağına kavuşması, dünyada ilk defa 1989 yılında meydana gelmiş ve ilk internet sitesi 1991'de dolaşıma girmiştir. İlk siber saldırının ise bu gelişmelerden önce 1988[109] yılında yapıldığı aktarılmaktadır.[110] Bugün için siber saldırılar her türlü bilişim sistemi ve her türlü ağ yapısı için tehdit oluşturmaktadır. IoT ağları ile bilgisayar ağları, Bluetooth ile internet altyapısı, araç bilgisayarları ile akıllı televizyonlar veya devasa SCADA sistemlerinden her biri an

---

[105] Ulaştırma ve Altyapı Bakanlığı 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda ise siber olay, ''*bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilgi/verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulması* şeklinde, siber saldırı ise *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 işlemler*'' şeklinde tanımlanmaktadır.

[106] Şeref SAĞIROĞLU 2018, age. s. 24.

[107] Bu konuda detaylı bilgi için bkz. Yunus Emre GÜL (2021), *Savaş Hukuku 2.0 Siber Saldırılar ve Hukuk*, Hukuk Akademisi, İstanbul, s. 32, 33, 34 vd.

[108] Yunus Emre GÜL 2021, age. s. 76, 77, 78.

[109] Aşağıda 1988 tarihinden daha önce yapılmış bir kısım hacking faaliyetlerinden örnekler aktarılmıştır. Lakin şüphesiz ki 1988 tarihi de siber saldırılar açısından erken bir tarihtir.

[110] Suraj GANGWAR ve Vinayak NARANG (2020), ''A Survey On Emerging Cyber Crimes and Their Impact Worldwide'', İçinde, *Encyclopedia of Criminal Activities and the Deep Web*, , ss. 23-36, IGI Global, USA, s. 24.

be an siber saldırılara maruz kalmaktadır. Aşağıda hacking yöntemleri açıklanırken detaylandırılacak olan bu saldırılar çok farklı şekillerde ve çok farklı amaçlarla gerçekleştirilebilmektedir.[111] IP kameraya sızan kıskanç bir eski sevgilinin böyle bir saldırıyı gerçekleştirmesi mümkün olduğu gibi aynı faaliyet bir siyasetçi aleyhine şantaj yapmak için de kullanılabilir veya ülke güvenliğini tehdit amacıyla terörist faaliyetlere araç olabilir. Büyük bir fabrikanın SCADA sistemine rakip bir firmanın veri sızdırma amacıyla yetkisiz olarak erişerek çeşitli işlemlerde bulunması salt ticari sırların ihlaline sebep olabileceği gibi saldırı sonucu sistemler zarar görebilir ve belki de saldırı bir çevre kirliliği felaketiyle sonuçlanabilir.[112]

Gerek fiil gerek amaç ve gerekse failler yönünden geniş bir yelpazeye sahip olabilen siber saldırılardan geçmişte gerçekleştirilmiş ve belirli bir üne kavuşmuş olan bir kısmını tezin bu başlığı altında örnek göstermek faydalı olacaktır. Örneğin, ABD tarihindeki ilk geniş çaplı siber saldırı örneklerinden biri ‘’moonlight maze‘’ olarak adlandırılan olaydır. Bu olayda üniversiteler, kritik altyapı tesisleri ve ordu gibi önemli noktaların veri trafiği ve veri tabanlarındaki bilgileri iki yılı aşkın süredir çalan bir spyware yazılımı tesadüfen 1998 yılında fark edilmiştir.[113] 2000 yılında Avustralya'daki atık kontrol sisteminin SCADA sistemine sızılmış, sistemin işleyişi bozularak atıklar doğaya salınmış ve nihayetinde de büyük bir doğal felakete sebep olunmuştur. 2010 yılında İran'ın nükleer enerji santralinde yer alan SCADA sistemlere Stuxnet worm sızdırılmış ve bu malware sistemin işleyişini bozarak göstergeleri etkilemiş, nihayetinde çok ciddi bir felaketin eşiğinden dönülmüştür.[114] 2016 yılında doğrudan bankadaki iç ağa sızılarak, Bank of Bangladesh'in SWIFT sistemine erişilmiş ve sistemin yetkisiz biçimde kullanılması sonucu çok ciddi bir haksız para transferi sağlanmıştır.[115] 2017 yılında WannaCry olarak adlandırılan bir malware, küresel çapta yüzbinlerce sisteme yayılmıştır. Kriptolanan veriler karşılığı fidye olarak

[111] Para ve veri hırsızlığı, botnet ağı oluşturmak, arka kapılar oluşturmak, paranın aklanması, dolandırıcılık, istismar faaliyetleri, yasak materyallerin satışı ve sair hususlar, EUROPOL'ün bilişim suçlarının işlenme amaçlarını açıklarken kullandığı örneklerdir. Bu konuda bkz. EUROPOL, Cybercrime, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime, (ET: 02.03.2022).

[112] Kritik altyapılara ve bu noktalardaki SCADA sistemlere yapılan siber saldırıların ciddi doğa felaketlerine sebep olabileceğine/olduğuna dair ayrıntılı açıklamalar için bkz. Semih Töner ŞEN 2021, age. s. 139.

[113] Semih Töner ŞEN 2021, age. s. 137.

[114] Muhammet KARACA (2019), *Kritik Altyapılara Yönelik Bilişim Suçları; Türkiye ve AB Uygulamaları*, İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, İstanbul, s. 39, 40, 41 vd.; Semih Töner ŞEN 2021, age. s. 141, 146, 147.

[115] Cemal ARAALAN (2021), *Teknik ve Hukuki Boyutlarıyla Elektronik Ödeme Sistemlerinde Siber Güvenlik*, Seçkin, Ankara, s. 89.

ele geçirilen miktar az olsa da bu saldırının ünü, yayıldığı sistemlerin sayısal fazlalığından kaynaklanmıştır.[116] Devlet destekli olduğu düşünülebilecek komplike siber saldırılara örnek olarak ise Kuzey Kore ile ilgili çektikleri komedi filmi sonrası Sony firmasının veri tabanlarına bir şekilde sızılarak buradaki bilgilerin ifşası verilebilir. IŞİD'in gerçekleştirdiği terör saldırısı şeklindeki bir siber saldırıda ise Fransız kamu medya kanalı olan TV5'in hem televizyon hem internet yayınları kesilmiş, siteler ele geçirilerek Hilafet yazısı paylaşılmış ve sosyal medya hesapları ele geçirilerek buradan terörist paylaşımlarda bulunulmuştur.[117]

2.2.2. Hacking Kavramı

Hukuk doktrininde dar anlamdaki bilişim suçlarının tipikliği içinde kalan fiillerin siber saldırılar olarak adlandırıldığı, bilişim ve ağ teknolojileri ile siber güvenliğe dair spesifik kaynaklarda ise siber saldırıların en geniş boyutuyla çatı bir kavram olarak ''hacking faaliyetleri'' şeklinde isimlendirildiği yukarıda zikredilmişti. Bu çatı kavram, dar anlamda bilişim suçlarına konu olmayan faaliyetleri de içerisinde barındırmaktadır. Örneğin internet aracılığıyla yapılan sosyal mühendislik faaliyetleri ve phishing uygulamaları sırasında dar anlamdaki bilişim suçlarına konu hareketler genellikle gerçekleştirilmez. Yine hedef sistem hakkında bilgi toplamak ve örneğin muhtemel kullanıcı şifrelerini açık kaynaklardan öğrenmek ya da hedef sisteme veri paketleri göndererek açık portlarını taramak gibi faaliyetler de herhangi bir suçun tipikliği içerisinde kalmamakla birlikte, bunlar geniş anlamda hacking kavramına dahil eylemlerdir.

Hacking kavramına dair literatür ve doktrinlerdeki genel algı, bilişim sistemlerine karşı yapılan saldırılar, sızmalar ve sair faaliyetler yönünde gelişmiştir. Ancak hack ve hacking kavramını bambaşka bir yönüyle daha algılayan ikinci bir literatür daha bulunmaktadır. Salt bilişim teknolojileri literatürünün teknik kısmında hack ve hacking, mevcut bilişim teknolojilerinin kurcalanarak geliştirilmesine ve/veya bilişim alanında yeni teknolojiler üretilmesine yönelik faaliyetler olarak da algılanır. Örneğin Kaspersky Bilişim Teknolojileri Ansiklopedisi'nin ''Hack'in Kısa Tarihi'' başlıklı bölümü, 1947'de transistörün icadından başlayarak 1968 ve 1969'da işlemci

[116] Güzin ULUTAŞ (2019), ''Siber Güvenlik'', İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 2, Siber Güvenlik ve Savunma-Problemler ve Çözümler*, Ed. Şeref Sağıroğlu, Mustafa Şenol, ss. 87-101, Grafiker, Ankara, s. 94, 95.
[117] Semih Töner ŞEN 2021, age. s. 147, 148, 149.

üreticilerinin kurulması ve 1993'te Mosaic'in kullanıma sunuluşu gibi olayları aktarmaktadır. Ancak aynı bölümde siber saldırı yönüyle hacking olaylarına ve örneğin 1983'te Arpanet'e yapılan sızmaya, 1984'te NASA ve ABD Savunma Bakanlığı'nın hacklenmesine, 1994'te Citibank'ın hacklenmesine ve sair önemli hacking eylemlerine de yer verilmektedir.[118] Hacking kavramının bugün için genellikle benimsenmeyen üçüncü bir algılanışı ise kendilerini hacker olarak tanımlayan ilk bilgisayar meraklılarının oluşturduğu Jargon/Hacker'ın Sözlüğü belgesinde yer almaktadır.[119] İlgili sözlüğün hack ve hacking ile ilişkili sözcükleri tanımlarken, bu kavramları genel olarak bilişim sistemlerinden bağımsız biçimde, salt bir durumun ''daha iyi ve/veya daha kullanışlı'' hale getirilmesi şeklinde açıkladığı görülmektedir.[120]

Hacking kavramı içerisinde müspet ya da menfi, hukuka uygun ya da aykırı pek çok faaliyeti barındıran geniş bir kavramdır. Geçmişi çok öncelere uzanan hackingin öncül spesifik örneği, bugünkü örnekleri TCK md. 243/4'ün tipikliği içerisinde kalan telgraf hatlarına sızılarak aradaki veri trafiğinin dinlenmesine dair 1903 yılındaki sniffing olayı olarak verilmektedir. Yine Turing'in geliştirdiği bilgisayarı ile Naziler'in Enigma cihazının kriptosunu kırması da ilk spesifik hacking örnekleri arasında gösterilmektedir.[121]

Hackingin pek çok uygulama alanı mevcuttur.[122] Ülkelerin iç hukukuna uygun hacking faaliyetlerine örnek olarak, iç hukuka dayanılarak gerçekleştirilen istihbarat amaçlı faaliyetler verilebilir. İkinci olarak ülkeler tahrip edici amaçlarla da savaş/çatışma hukukuna uygun biçimde resmi kanallarla hacking faaliyetlerine başvurabilirler.[123] Üçüncü olarak pek çok ülkede yetkililer, adli bilişim amaçlı hacking faaliyetleri gerçekleştirmektedir. Türk hukukunda bu yönde dayanak bir kanun normu bulunmasa da iç hukuka uygun hacking yöntemlerine başka bir örnek olarak, Alman Ceza Muhakemesi Kanunu md. 100/b'deki online arama düzenlemelerine dayanılarak bilişim sistemlerinin resmi görevliler tarafından uzaktan hacklenmesi verilebilir.

---

[118]Kaspersky Bilişim Teknolojileri Ansiklopedisi, *Hack'in Kısa Tarihi*, https://encyclopedia.kaspersky.com/knowledge/a-brief-history-of-hacking/, (ET: 02.03.2022).
[119] Bu sözlük ve öncül ya da ardıl dokümanları hakkında detaylı bilgi için bkz. Wikipedia, Jargon File, https://en.wikipedia.org/wiki/Jargon_File, (ET: 02.03.2022).
[120] *The New Hacker's Dictionary Version 4.2.2* (2012), Emereo Pty Limited.
[121] Gökhan USTA 2019, age. s. 31, 32.
[122] Siber saldırıların kaynaklarını beşe ayıran USOM'a göre bu kaynaklar; siyah şapkalı hackerlar, içeriden gelen saldırılar, hacktivist eylemler ve istihbarat kurumlarının hacking faaliyetleridir. Bkz. USOM (2014c), *Siber Güvenliğe İlişkin Temel Bilgiler*, s. 7, 8.
[123] Gökhan USTA 2019, age. s. 29.

Aşağıda detaylı olarak açıklanacak hacktivist faaliyetlerden bir kısmının da Avrupa İnsan Hakları Sözleşmesi nazarında hukuka uygun olması ve protesto hakkı sınırlarını aşmaması mümkündür.[124] Önleme amacıyla yapılan ve gerekli rızaların alındığı sızma testleri ve siber güvenliğe dair normlar kapsamında aktif savunma amacıyla gerçekleştirilen hacking faaliyetleri de hukuka uygun örneklerdendir.

Hukuka uygunluk sebeplerinin tecellisi sonucunda iç hukuk nazarında meşru sayılacak faaliyetler dışında, hacking kavramının karanlık boyutu ve hukuka aykırı alanı ise evvela maddi ceza hukukunun kapsamına giren ve belirli suçların tipikliği içinde kalan hacking faaliyetleridir. Bu tür hacking faaliyetlerini tekil gerçek kişiler veya suç örgütleri gerçekleştirebileceği gibi ülkelerin resmi birimleri de gerçekleştirebilir. Somut bir hukuki dayanak olmaksızın bilişim sistemlerindeki verilerin Pegasus Spyware örneğinde olduğu gibi ele geçirilmesi bu duruma örnektir. İkinci olarak siber terörizm olarak adlandırılan ve terör örgütlerinin terörist faaliyetleri dahilinde gerçekleştirdikleri hacking faaliyetleri de bu noktada örnek gösterilebilir.[125] Hukuka aykırı faaliyetler hacktivist amaçlarla, salt şahsi öç alma amacıyla, şantaj veya bilgi casusluğuna ya da sair çok farklı amaçlara yönelik gerçekleştirilebilir. Örneğin TCK md. 243/1'de yer alan bilişim sistemine yetkisiz erişim suçunun ASS'deki karşılığı olan ikinci maddeye dair ASS'nin Açıklayıcı Raporu'nda, sisteme yetkisiz erişimi nitelemek için ''hackleme'' kavramı kullanılmıştır.

İşte hackingin bu ''hukuka aykırı'' boyutu, hacking kavramına esas ününü kazandıran ve bu faaliyetlerin günümüzde ''hacking'' olarak adlandırılmasına sebep olan boyuttur. Genel olarak bir hukuka uygunluk sebebinin bulunmadığı bu tür hacking faaliyetlerinin hukuka aykırılığına dair bir tartışma söz konusu olmasa da geçmişten beridir hackingin bu boyutunun ''etik açıdan'' menfi bir faaliyet alanı olup olmadığı hep tartışılmıştır.

---

[124] Council of Europe, Toplantı ve Dernek Kurma Hürriyetine Dair Taslak Rapor, s. 18, 19, 20; Serkan BÜYÜKÇAĞLAR (2013), *İnternet'te Sivil İtaatsizlik*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü İnsan Hakları Hukuku Yüksek Lisans Tezi, İstanbul, s. 59, 60.

[125] ''*... siber terörizm kavramı ise siber ve terörizm terimlerinin birleşimi ile; terörist faaliyetlerin siber alan kullanılarak gerçekleştirilmesi ya da terör örgütlerinin siber alanı araç olarak kullanmaları olarak tanımlanabilmektedir*. '' Semih Töner ŞEN 2021, age. s. 26.

2.2.2.1. Hukuka Aykırı Hacking Faaliyetlerinin Etik Boyutu

Doktrinde bilişim sistemleri ile ilişkili hack ve hacking kavramlarının MIT'deki(*Massachusetts Teknoloji Enstitüsü*) öğrencilerin üniversitedeki bilgisayarlara dair yaptıkları keşif, iyileştirme ve geliştirme faaliyetleri ile oluştuğu yönünde görüşler mevcuttur.[126] Kaspersky Bilişim Teknolojileri Ansiklopedisi'nde MIT öğrencilerinin bu faaliyetlerinin başlama tarihi olarak 1969 verilir.[127] Hacking kavramının bilişim sistemleri üzerinde hukuki bir yetki sahibi olmaksızın bu sistemler üzerinde işlemler gerçekleştirme veya sistemlere zarar verme boyutuyla eşdeğer hale gelmesi durumunun ise John Draper'ın 1970'lerdeki phreaking olayları haricinde esas olarak 1980'lerde ortaya çıktığı belirtilir.[128]

1980'lerde bilişim sistemlerine yönelik hacking faaliyetleri, günümüzdeki kadar karanlık ve suç ile özdeşleşmiş bir algı yaratmıyordu. Bu dönemde hukuka aykırı olsa bile müspet amaçlarla, bilginin ve siber uzayın özgürlüğü düşüncesiyle gerçekleştirilen, bilişim sistemlerini keşfetmeyi ve geliştirmeyi hedefleyen fiiller yoğunluktaydı ve gizliliğe saygı, iletişim hakkı ile zarar vermemeyi önceleyen bir hacker etiği mevcuttu.[129] Zarar verme, bilgi hırsızlığı, dinleme, dolandırıcılık, fidye talebi ve sair menfi amaçlı hacking faaliyetleri çoğaldıkça ve hacking kavramı suç örgütleriyle anılmaya başladıkça, hacker etiği çok geçmişte kalmış ve hacking kavramı karanlık, suç odaklı bir anlama bürünmüştür.[130]

Robin Hood'un hukukçu gözüyle bakıldığında bir hırsız lakin farklı gözle bakıldığında bir kahraman olarak algılanacağı açıktır. Hukuka aykırı olarak gerçekleştirilen hacking faaliyetlerinde de aynı durum mevcuttur. Hukuken açıkça suç olan bazı hacking fiilleri ve özellikle hacktivist faaliyetler, küresel toplum yönünden kimi zaman etik bir sorun doğurmamakta ve hatta alkışlanabilmektedir. Ancak bilinmesi gerekir ki hukuk yalnızca teorik kurallardan ibaret olmayıp, toplumsal yaşamın uyulması gereken değerlerini teşkil eder. Nasıl ki çoğunluk bir kimsenin ölmesini istediğinde bu kişinin öldürülmesi olması gereken etik değerler açısından

---

[126] Gökşin AKDENİZ (2013), ''Hacker Etiği'', İçinde, *Hack Kültürü ve Hacktivizm*, ss. 9-16, Alternatif Bilişim, İstanbul, s. 10, 11; The Evolution of Hacking, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/, (ET: 02.03.2022).
[127] Kaspersky Bilişim Teknolojileri Ansiklopedisi*, Hack'in Kısa Tarihi.*
[128] Gökhan USTA 2019, age. s. 31.
[129] Serhat ÇOBAN (2020), ''Hackerlık Kavramı, Modeller ve Medyada Hackerlığın Sunumu''*, Bilişim Teknolojileri Online Dergisi*, C. 11, S. 40, ss. 43-64, s. 48, 49; Gökşin AKDENİZ 2013, age. s. 12, 13.
[130] İbrahim ÖZKAN (2019), *Siber Saldırıların Ekonomik Boyutu*, Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü İktisat Anabilim Dalı Yüksek Lisans Tezi, Bilecik, s. 4, 5; Gökhan USTA 2019, age. s. 30 / Şeref SAĞIROĞLU 2018, age. s. 31, 32.

meşru sayılamayacak ise hackingin de menfi-müspet amaçlı eylemler ayrımından tamamen çıkartılıp, hukuk sistemlerinin meşru kabul ettiği değerler ekseninde değerlendirilmesi ve olması gereken bir yapıda da yalnızca hukuka uygun hacking faaliyetlerinin olumlu karşılanması gerekir.

2.2.2.2. Hacker

Temelde bir önceki başlık altında açıklanan hacking faaliyetlerini gerçekleştiren kişiler ‘’hacker‘’ olarak adlandırılabilir. Günlük kullanımda da durum böyledir. Doktrinde ise hackerların; siyah şapkalı hacker, gri şapkalı hacker, beyaz şapkalı hacker, hacktivist, phreaker, cracker, script kiddie, lamer, siber terörist, ajan hacker, devlet destekli hacker ve sair şekillerde ayrıma tabi tutulduğu görülmektedir.[131] Bir kısım azınlık görüşüne göre ise yalnızca kötü niyetli eylemleri gerçekleştirenlere hacker denilmelidir.[132] TDK Sözlük'te kötü niyetli hackerlar bilgisayar korsanı olarak adlandırılmış ‘’*Bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse*‘’ şeklinde açıklanmıştır. Zıt yöndeki bir kısım azınlık görüşüne göre ise hackerlar tamamen zararsız işler yapan bilişim uzmanları, crackerlar ise zarar verenler olarak açıklanmaktadır.[133]

Yukarıda aktarıldığı üzere hacking kavramı zaman içinde gelişmiş, kapsama alanı genişlerken algılanışı ise kötümserleşmiştir. Bu sebeple artık sistemlerin geliştirilmesi ile sızma yahut zarar verme faaliyetleri yönünden bir ayrıma gidilerek, hacking-cracking ve sair kavramların güncel açıklamalarda yer almasını doğru bulmuyoruz. Zira artık literatürde cracking ancak bir açıklama cümlesinde, hacking ise kaynakların başlıkları dahil tüm içeriğindeki egemen kavram olarak yer almaktadır. Öyleyse çatı kavram olarak hacking faaliyetlerini gerçekleştiren herkesin hacker olarak adlandırılması ve ayrıca hackerlar arasında uzmanlık seviyelerine göre lamer ve scpirt kiddie gibi ayrımlara da gidilmemesi gerektiği düşünülmelidir.

Böylelikle nihai olarak hacking faaliyetlerinde bulunan hackerları beş temel alt kategoriye ayırmanın doğru olduğunu düşünüyoruz. Bunlar; istisnai durumlar haricinde bir hukuka uygunluk sebebi bulunmaksızın suç normlarının objektif

[131] İbrahim ÖZKAN 2019, age. s. 6, 7, 8, 9 vd.; İlker KARA (2015), ‘’Hacking(Yetkisiz Erişim) ve Hukuki Boyutu‘’, *Leges Hukuk Dergisi*, Kasım 2015, ss. 29-40, s. 32.
[132] Türkay HENKOĞLU (2014), *Adli Bilişim-Dijital Delillerin Elde Edilmesi ve Analizi*, Pusula, İstanbul, Giriş Bölümü s. 16, 17.
[133] Hamza ELBAHADIR (2021), *Hacking Interface*, Kodlab, Ankara, s. 8.

tipikliğine konu faaliyetleri gerçekleştiren siyah şapkalı hackerlar,[134] içeriğinde siber güvenlik uzmanlarının, adli bilişim-kolluk-istihbarat-askeri birimlerde görev yapanların bulunduğu ve hacking faaliyetlerini hukuka uygun olarak gerçekleştiren etik/beyaz şapkalı hackerlar, aktivist amaçlar ile hacking faaliyetlerinde bulunan hacktivistler ve nihayetinde de terör eylemi olarak hacking faaliyetlerinde bulunan siber teröristlerdir.

2.2.2.3. Hacktivizm

Esas itibariyle kültürel ve düşünsel bir felsefe olan hacktivizmin, hacking kavramı içerisinde ayrı bir önem arz ettiğini söylemek mümkündür. Hackingin masum görünen yüzü olan ‘’kullanışlı hale getirme-geliştirme‘’ faaliyetleri ve bu faaliyetleri gerçekleştiren bilişim teknolojisi tutkunu uzmanların, teknolojinin gelişimi ve teknik bilginin özgür dolaşımına dair bir felsefeyi benimsedikleri yukarıda zikredilmişti. Hacktivistler ise bilişim teknolojilerinin gelişimi ya da özgürlüğü ile direkt olarak ilgilenmezler. Açıklaması,

> ‘’*Sosyal, politik veya diğer konularda farkındalığı artırmak için siber saldırıların kullanılmasıdır. Terim, "hack" ve "aktivizm" kelimelerinin birleşimidir. Geleneksel siyah şapkalardan farklı olarak, bilgisayar korsanları genellikle finansal veya diğer kazançlardan başka amaçlara sahiptirler*.‘’[135]

şeklinde yapılan hacktivizmde esas olan, yaşamın her alanına konu meselelerdir.

Hacktivist eylemlerden büyük bir kısmı insan hakları ve daha çok anonim internet kullanımı ile ifade ve bilgiye erişim hakkının tecellisine yönelirken, sair eylemler; karşıt politik fikirlerin yayılmasına, iktidarların yıpratılmasına, sübjektif olarak meşru görülmeyen durumların ortadan kaldırılmasına veya sınırsız özgürlükte bir internet ve bilgiye erişim adına sivil itaatsizlik ve hatta anarşiye varan boyutlarda olabilmektedir.[136] Hacktivist felsefenin anonimliği önceleyen boyutu, hacktivist

---

[134] Siyah şapkalılar genellikle kötü amaçlı veya yetkisiz olarak hacking faaliyetlerini gerçekleştirenler olarak nitelendirilir. Bkz. Türkay HENKOĞLU 2014, age. s. 167; Erhan SAYGILI (2018), *Web Uygulama Güvenliği-Hacking Yöntemleri*, Dikeyeksen, İstanbul, s. 3.

[135] Kaspersky Bilişim Teknolojileri Ansiklopedisi, Hacktivizm, https://encyclopedia.kaspersky.com/glossary/hacktivism/, (ET: 02.03.2022).

[136] Hacktivistlerin devlet veri tabanlarında saklı olan gerçek bilgileri, bilgi edinme hakkına sahip olduğunu düşündükleri toplumla paylaşma amacı güttükleri ve politik görüşlerini ortaya koymak adına siber faaliyetlerde bulundukları yönünden ayrıca bkz. Murat Volkan DÜLGER 2022, age. s. 189, 190 / Hacktivizmde, hacking eylemlerinin politik veya sosyal sonuçlara ulaşmak amacıyla yapıldığı yönünde bkz. Elif KARA (2013), *Toplumsal Hareketlerin Dönüşümü ve Modern Bir Toplumsal Hareket Olarak Hacktivizm: Anonymous ve RedHack Örnekleri*, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Antalya, s. 47 / Ayrıca bkz. Türkay HENKOĞLU 2014, age. s. 168; Filiz AYDOĞAN BOSCHELE ve Özlem ÇETİN ÖZTÜRK (2017), ‘’Dijital İletişim Teknolojileri ve Toplumsal

eylemlerin anonim şekilde yapılabilmesine katkı sağlıyor olsa da hacktivizmde anonimliğe dair temel amaç, bilginin ve siber uzayın anonimliği ile devletlerin gözetiminden tamamen bağımsız bir internetin olması gerektiğidir. Adli bilişim faaliyetlerini sekteye uğratabilse ve/veya kara paranın aklanması gibi olumsuz sonuçları olsa da hacktivizmin bu yönü pek çok faydalı keşfe yol açmıştır. Örneğin Cypherpunk hareketinin çabalarıyla özel kişilerin kriptolu veri trafiği yapabilmesinin, anonim para aktarma cüzdanlarının ve en önemlisi de kripto para sistemlerinin doğuşuna hacktivist felsefe ön ayak olmuştur.[137] Ayrıca eklemek gerekir ki Anonymous gibi hacktivist grupların geçmişte çocuk pornografisine karşı ciddi mücadeleleri de bulunmaktadır.[138]

Bir hacktivist eylemin müspet olup olmadığı göreceli bir kavram olup, bu tezde üzerinde durulması gereken temel mesele hukuki zemindeki meşruluktur. Öyleyse bir hacktivist grubun eyleminin konusu suç işlemeyi ya da kanunlara uymamayı tahrik edecek hukuka aykırı unsurlar içermediği sürece, toplumun geneli tarafından olumsuz görülen bir konuyu över nitelikte de olabilir. Örneğin liberal bir toplum yapısında, özel mülkiyetin kaldırılmasının ve devletin tüm mallara el koymasının toplumsal açıdan daha faydalı olacağına dair bir eylem menfi görülebilir. Fakat bu menfilik, eylemin direkt olarak hukuka aykırı olmasını sağlamaz. Böyle bir hacktivist eylemi hukuka aykırı kılacak olan, eylemin gerçekleştirilme metotlarıdır ve bu sebeple hacktivist eylemler de şartları taşıyor ise hukuka uygun olabilirler.[139]

Hackingin aktivizm kavramı ile birleşmesi ve siber uzaydaki aktivist eylemlerin genel manasıyla hacktivizmi oluşturduğunu söylemek mümkündür. Hatta bu yönüyle DoS/DDoS saldırıları hacktivizm amaçlı yapıldığında oturma eylemlerine benzetilerek ‘’sanal oturma eylemleri‘’ şeklinde nitelendirilmektedir.[140] Protesto amacıyla ve sanal oturma eylemi şeklinde gerçekleşen her hacktivist eylem hukuka uygun sayılamayacak ise de bu tür eylemlerde kalıcı zarar verme amacı güdülmeden, sistemin işleyişi aksatılarak toplumsal mesajlar verilmeye çalışılır. Örneğin geçmişte

---

Hareketler Bağlamında Hacktivizm‘’, Üsküdar Üniversitesi Sosyal Bilimler Dergisi, S.5, ss. 429-452, s. 442, 443, 448; Serkan BÜYÜKÇAĞLAR 2013, age. s. 58.

[137] Timothy C. (1994), *Kripto Anarşi ve Sanal Topluluklar*, ABD, https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html, (ET: 02.03.2022); Dion Dalton-BRIDGES (2020), *A Brief History of The…Cypherpunks*, Medium.org, https://medium.com/the-capital/a-brief-history-of-the-cypherpunks-31ae447a14f, (ET: 02.03.2022).

[138] Jamie BARTLETT (2020), *Dark Net*, Çev: Yasin Konyalı, Timaş, İstanbul, s. 139, 140.

[139] Ayrıca bkz. Avrupa Konseyi, Toplantı ve Dernek Kurma Hürriyetine Dair Taslak Rapor, s. 18, 19, 20.

[140] Sanal oturma eylemleri ve bunlara dair tarihten örnekler için bkz Elif KARA 2013, age. s. 57, 58.

dünyanın dört bir yanından yaklaşık 450.000 kişinin katıldığı bir DDoS saldırısı, WTO'nun sistemlerinin işleyişini geçici olarak aksatabilmiştir.[141] Bununla birlikte, hacktivist eylemler geçmişte nadir olarak barışçıl protestolar içerisinde sistemin işleyişini geçici olarak aksatacak şekilde yapılmıştır. Hacktivizmin tarihinde daha çok politik ve/veya sosyal amaçlarını gerçekleştirmek ya da toplumsal bir mesaj vermek kaygısı güden eylemcilerin, yıkıcı ve zarar verici faaliyetleri mevcuttur.[142]

2.2.2.4. Spesifik Bir Saldırı Tipinden Bağımsız Olan Temel Hacking Kavramları

2.2.2.4.1. Güvenlik Açıkları ve Önleyici Çözümler

Güvenlik açığı, temel olarak bilişim sisteminin ağ üzerinden ya da fiziksel yollarla yapılacak çeşitli kötü niyetli işlemlere/saldırılara karşı savunmasız olduğunu belirtmek için kullanılan bir terimdir.[143] Güvenlik açığını ve hedef sisteme bağlantı sağlanabilecek bu korunmayan noktaları nitelemek için ''açık kapı'' terimi de kullanılmakta olup, bu terimin aktif bir eylem sonucu yaratılan ''arka kapılar'' ile tamamen farklı olduğunu vurgulamak gerekir. Güvenlik açıkları testler ile taranır ve siber güvenlik çözümleri ve/veya sistemdeki hataların düzeltilmesi ile kapatılırlar.

Hiçbir siber güvenlik önlemi bulunmayan bir sistemde kesinlikle güvenlik açıkları bulunacaktır. Ağa bağlı sistemlerde ağ üzerinden yapılacak işlemler, fiziki bağlantılarda da bağlantı noktaları üzerinden yapılacak işlemler eğer sınırlandırılmamışsa, bu durum evin kapısının gece açık bırakılmasına benzer. İşte bu bir güvenlik açığıdır. Bazen de siber güvenlik önlemleri olsun ya da olmasın, sistemin ya da siber güvenlik önlemlerinin işleyişinde bazı sıkıntılar doğabilir ve bu sıkıntılardan farklı güvenlik açıkları oluşabilir. Sistemlerdeki güvenlik açıklarının donanımlar ya da yazılımlardan kaynaklanması mümkündür. Hackerlar tarafından sistemlere fiziki yollarla erişmek genellikle çok zor olduğundan, güvenlik açıklarının yazılım kaynaklı oluşması daha büyük bir tehdit niteliğindedir.[144]

Güvenlik açıkları eğer sistemdeki yazılım ve/veya donanımların düzgün işlememesinden kaynaklanıyorsa, nadiren de olsa bu aksaklık göze çarpar ve açıklık

---

[141] Serkan BÜYÜKÇAĞLAR 2013, age. s. 59 / Bu yöndeki sair örnekler için ayrıca bkz. age. s. 56, 57, 58 vd.

[142] Bu yönde sair önemli örnekler için bkz. Pınar DEMİRKIRAN (2013), ''Hacktivizm'', İçinde, *Alternatif Bilişim, Hack Kültürü ve Hacktivism*, ss. 27-34, İstanbul, s. 33; Wikipedia, Hacktivism, https://en.wikipedia.org/wiki/Hacktivism, (ET: 02.03.2022).

[143] Wikipedia, Vulnerability, https://en.wikipedia.org/wiki/Vulnerability_(computing), (ET: 02.03.2022).

[144] BİLGEM (2021), *Sunucu Yönetimi Rehberi*, s. 32.

kapatılabilir. Lakin çoğu zaman sistemlerdeki aksaklıklar ancak detaylı analizler sonucunda ya da saldırı çoktan gerçekleştikten sonra fark edilirler. Gerek sistemdeki aksaklıklardan gerekse zaruri siber güvenlik çözümlerinin eksikliklerinden kaynaklı güvenlik açıklıklarının tespitinde, iki tip temel test yöntemi mevcuttur. Bunlardan birincisi, internet üzerinde çalıştırılan sistemlerin(*örn. web uygulaması*) açıklıklarını tarayan yazılımların kullanılmasıdır. Güvenlik açıklarını tarayan bu yazılımlar tarayıcılar ile entegre biçimde de çalışabilmektedir.[145] İkinci ve esas test yöntemi ise her türlü ağ yapısının, bu ağlardaki sistemlerin ve sistemler içindeki yazılım ile donanımların güvenlik açıklarını tarayan sızma testleridir. Sızma testlerinde sistemler üzerinde teste rıza gösterildikten ve gizlilik sözleşmesi ile sair prosedürler tamamlandıktan sonra, beyaz şapkalı hackerlar bu sistemleri hukuka uygun olarak hacklemektedir.[146] Sızma testleri, beyaz şapkalının sızma testinden önce sistem hakkında sahip olduğu bilginin boyutuna göre beyaz/gri/siyah kutu testler şeklinde üçe ayrılmaktadır. Beyaz kutuda hackerın elinde sistem yöneticisine eşdeğer derecede bilgi bulunmakta, gri kutuda hackera sistem ağındaki kullanıcılar kadar bilgi verilmekte, siyah kutuda ise hackerın sistem hakkında kendi çabalarıyla bilgi sahibi olması ve bu bilgiler üzerinden tam bir siyah şapkalı gibi hareket ederek açıklıkları bulmaya çalışması gerekir.[147] Bu iki test yöntemine ek olarak, sistemin değil lakin sistemde çalıştırılacak yazılımların veya sistemde yapılacak geliştirmelerin önce sandbox/test ortamında denenerek test edilmesi de olası güvenlik açıklarının oluşumunun önüne geçecek ya da mevcut güvenlik açıklarının ortaya çıkmasına katkıda bulunabilecektir.

Bazen güvenlik açıkları son kullanıcılar tarafından tam olarak müdahale edilebilir olmayabilir. Örneğin dışarıdan tedarik edilen sistem veya uygulama yazılımlarında, bulut çözümlerde ve hatta siber güvenlik çözümlerinde üretici/tedarikçiden kaynaklı güvenlik açıkları oluşabilir. USOM, 2014 yılından beri

---

[145] Erhan SAYGILI 2018, age. s. 166, 167, 168 vd.

[146] Mustafa Yasir ŞENTÜRK 2018, age. s. 3; Şeref SAĞIROĞLU 2018, age. s. 29, 30 / Sızma testleri, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik md. 3/1-ğ'de ''*Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen güvenlik testleri*'' şeklinde tanımlanmaktadır. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'ndaki tanımı ise ''*Bilişim sistemlerinin veya ağın güvenlik önlemlerini atlatmanın yollarını belirleme, sisteme sızma ve bu şekilde öncelikli sistem zafiyetlerini ve açıklıklarını belirlemeye yönelik test*'' şeklinde yapılmıştır. / Ayrıca bkz. Türk Standartları Enstitüsü (2014), *Sızma Testi Hizmeti Veren Personel ve Firmalar İçin Yetkilendirme Programı*, s. 7, 8.

[147] Beyaz.net, Black Box ve White Box Testi, www.beyaz.net/tr/guvenlik/makaleler/black_box_ve_white_box_testi.html, (ET: 02.03.2022); Türk Standartları Enstitüsü, a.g.b., s. 6.

bu tür güvenlik açıklarını sitesinde paylaşmaktadır.[148] Bu tür güvenlik açıkları genellikle üretici/tedarikçiler tarafından giderilir ve güncellemeler oluşturularak kullanıcıların bu güncellemeleri yüklemeleri vasıtasıyla açıkları kapatmaları beklenir. Ancak pekala içeriğine müdahale edilebilen açık kaynak yazılımlarda, bu güvenlik açıklarını kullanıcıların da kapatması gündeme gelebilir.

Güvenlik açıklarını oluşturacak siber güvenlik eksiklikleri, geniş kapsamlı olarak anlaşılmalıdır. Örneğin trojan niteliği taşımasa bile herhangi bir uygulamanın kamera, konum bilgisi ya da hafıza birimlerine kolayca erişebiliyor olması ve buna dair bir önlem alınmaması da bir güvenlik açığı sayılır.[149] İkinci olarak sisteme yetkili biçimde erişebilmek için hiçbir parolanın koyulmaması, konulan parolaların basit olması veya ağ erişimlerinde çok aşamalı yetki doğrulama ve bot kontrolü/captcha çözümleri olmaması da güvenlik açığı teşkil eder. Zira bu zayıflıklar saldırıların yapılabilmesini kolaylaştıracaktır. Üçüncü olarak, içeriden yapılacak veri sızıntılarına karşı sistemlerde bu sızıntıları önleyecek ve/veya raporlayacak şekilde; kriptografiye, yetkilendirmeye ve yedeklemeye dayalı olarak verilerin kaybını, silinmesini, çalınmasını önleme teknikleri olan DLP ve benzeri bir teknolojinin çalıştırılmaması da güvenlik açığı teşkil edecektir.

Güvenlik açıklarının oluşmasını sağlayacak dördüncü ve beşinci siber güvenlik eksiklikleri ise IDS-IPS çözümleri ve Firewall uygulamalarının kullanılmamasıdır. Bu üçlü genellikle birbirinin tamamlayıcısı konumundadır. IDS saldırıların tespitine, saldırı uyarılarına/alarmlara ve kötü niyetli trafiğe dair logların tutulmasına yönelik bir siber güvenlik çözümüdür. IPS ise saldırılara karşı mücadeleye ve örneğin kötü niyetli istemci trafiğini engellemek gibi savunmalara yönelik bir siber güvenlik çözümüdür.[150] Firewall uygulamaları ise dış ağdan gelen trafiğin, iç ağda yapılan trafiğin ve iç ağdan dış ağa gönderilen verilere dair trafiğin IP adresi-port bilgisi-MAC adresi-Alan Adı-URL ve benzeri bilgilere dayalı olarak filtrelenmesine dair güvenlik çözümlerini niteleyen çatı bir kavramdır. İstenirse firewall yapılarında paket filtreleme gerçekleştirilebilmekte ve veri paketleri incelenerek içeriğinde izin verilmeyen verileri barındıran trafikler de engellenebilmektedir. Firewall sistemleri ağdaki sistemler üzerinde veya ağa yönelik olarak tek bir sistem/sanal makine konumunda, routerlar

[148] https://www.usom.gov.tr/tehdit.html
[149] Ersin MASUM ve Refik SAMET (2018), ‘’Mobil BOTNET ile DDoS Saldırısı‘’, *Bilişim Teknolojileri Dergisi*, C. 11, S. 2, , ss. 111-121, s. 113.
[150] IDS ve IPS sistemlerin çalışma prensiplerine dair detaylı anlatım için bkz. Hamza ELBAHADIR 2021, age. s. 128, 129, 130 vd.

üzerinde veya ağ trafiğinin üzerinden geçtiği sair noktalarda çalıştırılabilirler.[151] Bu klasik şekliyle firewalların web sunucularda o sunucuya yönelen trafiğe dönük çalıştırılması da mümkündür. Fakat web sunuculara yönelik WAF çözümleri geliştirilmiştir. Web sunucularda çalıştırılan bu firewall tipi hem klasik firewall özelliği göstermekte hem de IPS gibi savunma yapabilmektedir.[152]

USOM; malware barındıran, phishing tehlikesi bulunan veya sair hacking araçlarını kullanan internet adreslerine dair bir ‘’zararlı bağlantılar listesi‘’ yayınlamaktadır.[153] Bu liste gibi küresel ölçekli bir çok liste bulunmakta olup, örnek bir firewall içerisinde kurulacak filtrenin, en basit haliyle LAN içerisinden bu bağlantılara yapılacak trafiğin engellenmesini sağlaması gerekir. Aksi halde bariz bir güvenlik açığı oluşacaktır. Yine sistemde IDS kurulmamışsa, saldırıya dair uyarılamayan yöneticinin saldırıdan haberdar olma ve savunma yapma şansı azalacak, bu da bir güvenlik açığı oluşturacaktır. Aynı durum IPS'nin eksikliği durumu için de geçerlidir.

Altıncı olarak, firewall çözümlerinden daha gelişmiş şekilde ağdaki trafik üzerinde yetki dağılımı ve filtreleme gerçekleştirebilen NAC çözümlerinin kullanılmaması da kısmen bir güvenlik açığı doğurabilir. Zira bu çözüm, hangi açığın sebep olduğu bilinmeyen *zero day attack* durumlarının önlenebilmesine yönelik kullanılabildiği için güvenlik açıklarıyla bağlantılıdır.[154] Yedinci olarak, anti virüs/malware yazılımlarının sistemde mevcut olmaması, çok basit ama ciddi bir güvenlik açığı oluşturacaktır. Sekizinci olarak kriptografik çözümler kullanılmaması, güvenlik açığı oluşturacaktır. Ağ içerisindeki veya internet üzerinden yapılan veri trafiği kriptolanmadığında, bu trafik doğru yazılım kullanılıyor ise tamamen izlenebilir/dinlenebilir. Sistemde depolanmış veriler kriptolanmadığında ise şifreler gibi önemli verilerin saldırganlar tarafından öğrenilmesi ihtimalinden kaynaklı bir güvenlik açığı gündeme gelecektir. Bu noktada veri trafiğine yönelik VPN'ler, veri dosyalarının kriptolanmasına yönelik ise hash+salting uygulamaları örnek verilebilir. Bir diğer kriptografik çözüm ise veri trafiğinin değil, veri trafiği içerisindeki veri dosyalarının ve örneğin bir mail'in PGP ve sair yazılımlar kullanılarak kriptolanmasıdır.

[151] BİLGEM (2017), *Güvenlik Yazılımı Tedariki Rehberi*, s. 3.
[152] Erhan SAYGILI 2018, age. s. 232.
[153] https://www.usom.gov.tr/zararli-baglantilar/1.html, (ET: 02.03.2022).
[154] Wikipedia, *NAC*, https://en.wikipedia.org/wiki/Network_Access_Control, (ET: 02.03.2022).

Yukarıda zikredilenler haricinde, eksikliği çeşitli güvenlik açıklarını doğurabilecek pek çok siber güvenlik çözümü mevcuttur. Siber güvenlik çözümleri yönünden belirtmek gerekir ki yukarıda zikredilen temel çözümler, genellikle ağ yapısında eş güdümlü çalıştırılırlar ve ancak bu şekilde sistemin bir güvenlik açığı vermemesi amaçlanır. Bu teknolojiler ayrı ayrı kurulup konumlandırılabileceği gibi içeriğinde çeşitli bütünleşik çözümleri barındıran donanım+yazılımlar bütünü şeklinde ‘’bütünleşik sistemler-birleşik tehdit yönetimi sistemleri‘’ de mevcuttur.

2.2.2.4.2. Keşif ve Arka Kapılar

Hackingin hedefi olan bilişim sistemleri genellikle ağ topolojisi içerisindeki tekil sistemler, bağlantı ekipmanları ve ağın külli halidir. Nadiren ise ağa bağlı olmayan tek bir sistem fiziki yollarla hacklenir. Bir hacking operasyonu, modellemelerde çeşitli aşamalara ayrılmaktadır. Bu doğrultuda en ünlü modelleme *Siber Ölüm Zinciri* olan yedi aşamalı anlatımdır.[155] Hangi modelleme olursa olsun, tüm anlatımlarda ilk aşama keşiftir. Tez içeriğinde basitçe aktarılabilecek ve diğer modellemelerin daha temele indirilmiş hali olan üç aşamalı anlatımda da hacking operasyonu, hedef sistemdeki IP-MAC-port bilgisi, işletim sistemi, ağ topolojisi ve çalıştırılan siber güvenlik uygulamalarına yönelik keşif ile başlar, hedef sistemlerdeki güvenlik açıklarının taranması ile devam eder ve nihayetinde veri hırsızlığı yahut zarar verme amacını gerçekleştirecek nihai fiiller gerçekleştirilir.[156]

Tez konusu ile bağlantılı olduğu için altını çizerek belirtmek gerekir ki bilişim sistemine erişmek ya da ağ trafiğine sızmak çoğu zaman hackingin nihai hedefleri arasında olup, bunlar genellikle keşfin konusunu oluşturmaz. Keşif, evvela sisteme erişmeyi ve/veya ağ trafiğini izlemeyi başarabilmek adına gerçekleştirilen faaliyetlerdir. Ancak örneğin LAN ağındaki bir sisteme erişilerek ağın topolojisi çıkartılabileceği, sistemdeki veri trafiği üzerinden IP-MAC-port bilgisi elde edilebileceği ve sair bilgiler ortaya çıkarılabileceği için keşif aynı zamanda ağdaki bir sisteme erişildikten sonra gerçekleştirilen faaliyetleri de konu eder.

Körlemesine operasyona başlaması akıllıca olmayacak olan hackerın yapacağı keşif, çok farklı yollarla gerçekleştirilebilir. Doktrinde hedef sisteme dair keşif yöntemleri pasif ve aktif olarak ikiye ayrılmaktadır. Pasif keşif, internet vasıtasıyla

[155] Detaylar için bkz. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, (ET: 02.03.2022).
[156] Gökhan USTA 2019, age. s. 73.

erişilen ve sair noktalardaki aleni bilgilerin edinilmesine yönelik faaliyetlerdir. Aktif keşif ise hedef sistem veya sistem ile bağlantılı herhangi bir sistem ile etkileşime geçilerek yapılan bilgi toplamadır.[157] Sisteme erişildikten sonra da keşif gerçekleştirilebileceğinden, bu ayrımı keşifteki ‘’ilk yöntem‘’ olarak açıklamak doğru olacaktır. Öyleyse keşifte ilk yöntem, ağdaki herhangi bir sisteme veya ağ trafiğine sızmadan, açık kaynaklardan ya da otomatik gerçekleşen veri alış-verişinden yararlanmaktır.[158] Bu noktada istisnai bir durum olan ve ‘’omuz sörfü‘’ olarak adlandırılan, parola gibi hacking için gerekli bilgilerin mağdurun fiziki olarak gözlenmesi sonucu elde edilmesi,[159] çöplerin karıştırılarak ya da sosyal mühendislik yöntemleriyle bilgi edinilmeye çalışılması gibi durumlar da sisteme erişilmeden yapılan keşif faaliyetlerine dahil edilebilir.

Açık kaynaklardan bilgi toplamak şüphesiz ki herhangi bir hukuka aykırılık barındırmaz. Bu tür yöntemlerde Google Hacking olarak adlandırılan ve basit arama araçları vasıtasıyla(*örn. ‘’index of‘’ eki ile*) yapılan Google taramaları ile hackingde faydalı olabilecek kişisel verilere ve/veya sistemlere dair bilgilere ulaşılmaya çalışılması gibi faaliyetler yer alır.[160] Özellikle alan adlarının sahipleri ve sunuculara dair bilgilere internet üzerinden kolayca ulaşılabilmektedir. Bunların dışında, sunucularda çalıştırılan işletim sistemi bilgisi de kimi zaman arama motorlarında çıkmaktadır. Örneğin alan adlarına dair WHOIS veri tabanındaki bazı bilgiler, bilgilerin gizlenmesine yönelik aktif bir eylemde bulunulmamışsa otomatik ve yasal olarak yayınlanır. Lakin kimi zaman intranetlerde kapalı olarak yer alması gereken veri tabanlarına dair URL’ler, ihmal sonucunda Google ve sair arama motorlarına açık hale gelebilir ve arama motorlarının örümcekleri bu veri tabanlarını da tararlar. İşte bu durum, açık kaynak taramanın kısmen etik olmayan boyutudur.

Veri alış-verişi yöntemiyle keşfe ise örnek olarak, basit bir IP sorgusu verilebilir. Örneğin kişi ping veya nslookup komutu ile sunucu IP’leri öğrenilmek istenilen alan adını kendi sistemine girerek hedef IP bilgilerine ulaşabilir.[161] Sisteme dışarıdan gönderilen veri paketlerine verilecek cevaplar, sistemin Macos, Windows, Linux yahut sair bir yazılım olduğunu da ele verebilir. Bu sebeple hedef işletim

[157] Erhan SAYGILI 2018, age. s. 84.
[158] Hamza ELBAHADIR 2021, age. s. 41, 42, 43, 44, 45 vd.
[159] Mustafa Yasir ŞENTÜRK 2018, age. s. 97.
[160] Sean Philip ORİYANO 2014, age. s. 115, 116.
[161] Gökhan USTA 2019, age. s. 74, 75.

sisteminin ne olduğunu öğrenmek için daima sisteme erişmeye gerek yoktur.[162] Hedef sisteme veri paketleri gönderilerek yapılan keşiflerde, bu yöndeki bilgi toplama faaliyetleri manuel şekilde yapılabileceği gibi karşıdaki sisteme dair yapıyı tarayacak yazılımlar da kullanılabilir.[163] Örneğin kablosuz ağlarda ağa dahil olmadan, ağ hakkındaki bir çok bilgi çeşitli yazılımlar kullanılarak elde edilebilir.[164]

Bilişim sistemine yetkisiz erişim suçu ile sisteme erişmeden yapılan keşif faaliyetlerinin bağlantısı önemlidir. Tekil bilişim sistemleri ve ağ yapıları, yukarıda da zikredildiği üzere olması gereken vaziyette en basit haliyle şifreleme ve firewall uygulamaları vasıtasıyla korunur. Bu sebeple bir sisteme yetkisiz olarak erişebilmek için evvela belirli bilgileri elde etmek gerekir. IP ve MAC adreslerine yönelik keşif, evvela hangi adrese saldırı yapılacağını bilebilmeyi sağlar. Ancak en önemlisi şudur, bu bilgiler taklit edildiğinde(*spoofing*) ve örneğin saldırgan sistemin IP ve MAC adresi ağa katılmaya yetkili sair bir sisteminkini taklit ederek değiştirildiğinde, firewall aşılabilir. Kullanılan portların bilgisi tespit edildikten sonra ise veri iletimi için hedef ile bağlantı kurulabilir.[165] Özellikle hedef sistemdeki şifrelemelerin aşılmasında gündeme gelecek olan brute force saldırılarından önce, denenecek kombinasyonlara dair nitelikli bir kütüphane oluşturmak için omuz sörfü, çöp karıştırma ve sosyal mühendislik aracılığıyla yapılan keşiften de önemli sonuçlar alınabilir. Ancak bunun ötesinde güvenliğe dair fiziki token ve e-imza gibi önlemler de alınmış ise bu yöntemler bunların da elde edilmesine veya sahtelerinin üretilmesine yönelik bir nevi keşif görevi görebilir. Tüm bu bilgiler kullanılarak da bilişim sistemine yetkisiz olarak erişmeyi sağlayacak bir hacking saldırısı gerçekleştirilebilir.

Sisteme yetkisiz olarak erişmeyi amaçlayan bir hacking saldırısı başarılı olduğunda, hacker daha sonra bu sisteme tekrardan erişebilmek ve bu sefer aynı yolları değil daha kolay bir yolu kullanabilmek için ‘’arka kapılar‘’ açar. Bu arka kapılar çeşitli yazımların ayarları değiştirilerek erişim izinleri verilmesi, bir takım portların açık bırakılması ya da doğrudan malware yüklenmesi şeklinde gerçekleşebilir. Hacker eğer sistemde daha kuvvetli değişiklikler yapmak ve/veya siber güvenlik çözümleri tarafından değişikliklerin bulunamamasını sağlamak istiyorsa, kendisine

[162] Hamza ELBAHADIR 2021, age. s. 73, 74 vd. / Ayrıca bkz. Onur AKTAŞ (2020), *Siber Güvenlik-Hacking Atölyesi*, Gazi Kitabevi, Ankara, s. 161, 162.
[163] Bu yönde ayrıntılı bilgiler için bkz. Gökhan USTA 2019, age. s. 86, 87, 88, 89, 90, 108.
[164] Bu konudaki detaylı örnekler için bkz. Besim ALTINOK 2021, age. s. 65, 66, 67 vd.
[165] Gökhan USTA 2019, age. s.101.

root/yöneticilik yetkisi veren rootkit türü malware yazılımları yükleyecektir.[166] Tüm bunlar arka kapı olarak adlandırılır ve özellikle bilişim sistemine yetkisiz erişim suçunun zincirleme biçimde işlenmesinde arka kapıların önemli bir işlevi mevcuttur.

2.2.2.4.3. Malware(*Zararlı Yazılım*)

Bazı yazılımlar; yüklendiği sisteme uzaktan bağlantı gerçekleştirilmesini sağlayabilir, sistemdeki çeşitli verileri kriptolayabilir, verileri bozabilir, sistemde kendiliğinden yayılabilir, yönetici izinlerini ele geçirebilir, mikrofona ya da kameraya erişebilir, sistemdeki çeşitli verileri belirli sunuculara otomatik olarak gönderebilir, ağdaki diğer sistemleri dinleyebilir, klavyenin ya da ekranın başka sistemlerden kontrol edilmesine ya da hareketlerinin görülmesine sebep olabilir. Tüm bu özellikler çeşitli yazılımlarda birlikte ya da ayrık olarak bulunabilmektedir. Bu tip yazılımlar, genellikle sistem yöneticilerinin ağdaki çeşitli makinelere kurduğu ve bu şekilde sistemleri kontrol edebilmeyi amaçladığı yazılımlardır. Bu yönüyle faydalı olan ve çoğu da bu amaçla geliştirilen yazılımlar, kötü amaçlara yönelik kullanıldığında ise faydalı değil ‘’zararlı‘’ olmakta ve zararlı yazılım/malware şeklinde nitelendirilmektedir.

Sistem/ağ yöneticilerinin kullanımına sunulanlar haricinde herhangi bir ‘’faydalı‘’ yazılım, içerisindeki bir kodun ve algoritmasının sunduğu özelliklerden dolayı spyware, keylogger veya sair bir malware özelliği gösterebilir. Bu durum tamamen yazılımın kodlanma biçimi ve algoritmasıyla ilgilidir. Örneğin işletim sistemi yazılımları, ürünü işleten Microsoft-Apple gibi hizmet sağlayıcıların gerektiğinde erişimi ve/veya güncellemesi için belirli açıklar bırakır. Aynı şekilde pek çok üründe üretici firmanın gerektiğinde sisteme erişilebilmesine yönelik fabrika ayarları bulunur. Bunlardan bir kısmı kullanıcı inisiyatifi ile devre dışı bırakılabilir ise de bu tür Jailbreak ve benzeri durumlar, sistemleri garanti kapsamından çıkartabilmektedir. Yine pek çok uygulama yazılımı, sisteme dair belirli yetki ve izinleri alarak çalışır. Ancak bu tür yazılımlar kötü niyetle çalıştırılmadıkları için malware olarak nitelendirilmezler.

[166] Erhan SAYGILI 2018, age. s. 7; Refik SAMET ve Ömer ASLAN (2018), ‘’Kötü Amaçlı Yazılımlar ve Analizi‘’, İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 1*, ss. 225-255, Grafiker, Ankara, s. 230; Wikipedia, Backdoor, https://en.wikipedia.org/wiki/Backdoor_(computing), (ET: 02.03.2022).

USOM malware tiplerini virüs, spyware, trojan, rootkit ve worm olarak ayırmıştır.[167] Bazı görüşlerde bu tipler arasında ransomware de sayılmaktadır.[168] Ek olarak keyloggerları malware tipleri arasında değerlendiren görüşler de mevcuttur.[169] Malware tiplerine dair en ayrıntılı sıralama ise EUROPOL'ün sıralamasıdır. Bu sıralamada botnet, rootkit, worm, trojan, file infector(*virüs*), backdoor trojan, ransomware, spyware, adware ve scareware yer almaktadır.[170] İşte malware kavramı, bu sayılan tiplerin özelliklerini barındıran yazılımlara dair çatı bir kavramdır.[171] Bu noktada bilinmesi gereken en önemli husus, bu sıralanan malware tiplerinin yazılımın ''özelliğini'' niteliyor oluşu ve bir zararlı yazılımın bu özelliklerden pek çoğunu bünyesinde bir arada bulundurabileceğidir. Örneğin bir malware hem virüs özelliği taşıyarak sisteme zarar verebilir hem solucan özelliği taşıyarak kendini kopyalayabilir ve/veya ağda yayılabilir hem trojan özelliği göstererek faydalı bir yazılımmış izlenimi vererek arka planda bu zararlı işlemleri yürütebilir ve hem de botnet özelliği göstererek sistemdeki bazı işlem izinlerini hackera verebilir. Aynı şekilde bir zararlı yazılım trojan özelliği göstererek faydalı bir yazılımmış izlenimi verebilir, spyware özelliği göstererek sistemdeki trafiği hackera aktarabilir ve aynı zamanda keylogger özelliği göstererek ekran ve klavye girdilerini hackerın izlemesini sağlayabilir. Yine bir yazılımın ransomware özelliği göstererek dosyaları kriptolaması, rootkit özelliği göstererek sistemde yönetici izinlerini hackera vermesi ve virüs özelliği göstererek, kriptonun fidye olmadan çözülmesi halinde tüm sisteme zarar verecek şekilde ayarlanması söz konusu olabilir.

Malware kavramı genel olarak hedef sisteme yüklenen zararlı yazılımları nitelemek için kullanılır. Örneğin hedef sisteme yüklenmeyen fakat hackingde kullanılan brute force yazılımları, tarayıcı yazılımlar, paket analiz yazılımları ''malware'' olarak değerlendirilmemektedir. Başka bir ayrım da zararlı kod ve

---

[167] USOM 2014c, age. s. 9.

[168] Poongodi THANGAMUTHU, Anu RATHEE, Suresh PLANİMUTHU ve Balamurugan BALUSAMY (2020), ''Cybercrime'', İçinde, *Encyclopedia of Criminal Activities and the Deep Web*, ss. 1-23, IGI Global, USA, s. 5; Cemal ARAALAN 2021, age. s. 94.

[169] Mesut UKŞAL (2015), *Mobile Forensics*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, s. 35.

[170] EUROPOL, *Cybercrime*, www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime, (ET: 02.03.2022).

[171] A. Nurdan SARAN (2019), ''Fidye Yazılımlar'', İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 3*, Ed. Şeref Sağıroğlu, ss. 227-240 Grafiker, Ankara, s. 227; Refik SAMET ve Ömer ASLAN 2018, age. s. 225; EUROPOL, Cybercrime / Bazı görüşlere göre malware ile virüsler farklı kavramlar olarak değerlendirilmektedir. Bkz. Semih Töner ŞEN 2021, age. s. 126.

malware ayrımıdır. Hackingde ve özellikle enjeksiyon saldırılarında, bir kısım kodlar da kullanılır. Örneğin bir web sitesindeki kodlar arasına zararlı kodlar enjekte edilerek, ziyaretçilerin sitedeki bir noktaya tıkladıklarında bilgisayarlarının otomatik olarak sitenin phishing amaçlı sahte ikizine yönlendirilmesi ve bu sayede şifresini bu sahte ikize girerek verilerinin çalınması sağlanabilir. Bu tür kodlar ile malware farklı hususlardır. Malware, sistemde yer kaplayan ve depolama birimlerinde barınan veri bütünü/yazılımlardır. Genellikle bu tür yazılımlar kendilerini gizliyor olsalar bile sabit hafıza birimlerinde barınırlar. Lakin uçucu hafıza/RAM'de barınabilen ve sistem kapatıldığında silinen malware türleri de mevcuttur.[172]

Aşağıda malware türü yazılımların bir kısım baskın özellikleri açıklanmıştır. Açıklananlar haricinde çeşitli özelliklerine veya kullanım amaçlarına göre bu tür yazılımlar değişik isimlendirmelere tabi tutulabilmektedir. Örneğin rootkit özelliği gösteren bir malware eğer DDoS atağında kullanılmak üzere köle bilgisayar ağı/botnet oluşturmak için kullanılıyor ise botnet yazılımı olarak isimlendirilebilmektedir. Aynı şekilde trojan özelliği gösteren bir mobil oyun aplikasyonu/uygulaması, hackerın sızabilmesi için arka kapılar bırakıyor ise RAT/backdoor trojan olarak isimlendirilebilir. Bu örneklerin çoğaltılması mümkün olmakla birlikte, işbu tez konusu açısından aşağıdaki temel özelliklerin bilgilendirme açısından yeterli olacağı değerlendirilmiştir.

2.2.2.4.3.1. Rootkit

Bilişim sistemleri üretilirken, sistemlerde üretici firmaların kullanıcı güvenliği ve ürünlerinin(*yazılım+donanım*) güvenliği için bazı fabrika ayarları bulunur. Bu fabrika ayarlarına konu işlemler, yönetici izni/root yetkisi alınmadan kullanıcılar tarafından gerçekleştirilemez. Örneğin bazı temel uygulama yazılımları root yetkisi alınmadan kaldırılamaz, bazı isimler dosyalara verilemez ya da bazı uygulama yazılımlarının çeşitli ayarları bu yetki alınmadan değiştirilemez veya sistemdeki temel bazı kodlara erişilemez yahut müdahale edilemez. Sistemin düzgün çalışmasını ve bilinçsiz kullanıcıları korumayı amaçlayan bu tür sınırlamaların bulunduğu bazı fabrika ayarlarının, kullanıcılar tarafından değiştirilmesine izin verilmiş olup sistem ayarlarından bunlar değiştirilebilmekte ve kullanıcı kendisine yönetici izni

[172] Teemu VAİSANEN, Lorena TRİNBERG ve Nikolas PİSSANİDİS (2016), *I Accidantally Malware – What Should I Do… Is This Dangerous*, The NATO Cooperative Cyber Defence Centre of Excellence, Talinn, s. 30.

verebilmektedir. Lakin bazı sınırlamaların değiştirilmesine izin verilmez. Üreticilerin koyduğu bu değiştirilmemesi gereken sınırlamalar şüphesiz ki kullanıcılar tarafından değiştirilebilir ve bu durum ürünün garantisini bozabileceği gibi hukuka aykırı durumlar da yaratabilir. İkinci olarak sistemlerde kullanıcıların yetkili olduğu ‘’yönetici‘’ konumu bulunur ve bir sistemdeki farklı yetkili kullanıcılardan biri yönetici konumunda olarak yalnızca belirli işlemleri gerçekleştirme yetkisine sahip olabilir. Örneğin bu şekilde yetkili olmayan bir kullanıcı sistem geçmişini silemez.

Rootkit yazılımlar diğer malware tiplerinin pek çok özelliğini bünyesinde barındırabilir. Örneğin İran'a yapılan saldırıda kullanılan Stuxnet hem bir virüs hem bir worm ve hem de bir rootkit özelliği göstermektedir.[173] Rootkit özelliğine sahip yazılımlara bu ismin verilmesinin nedeni, özünde yönetici yetkilerini ele geçirebilen bir yazılım olmasıdır. Tek bir rootkit bu işlemleri yapacak yetenekte olabileceği gibi ‘’kit‘’ adlandırılmasının yapılmasının nedeni olduğu üzere, birden fazla yazılımın birlikte işleyerek de bir rootkit oluşturması mümkündür. Yönetici izinlerini ele geçiren bir hackerın sisteme rootkit yükleyerek bu ayrıcalığını koruması mümkün olduğu gibi rootkit'in bu izinleri kendisinin elde etmesi de olanak dahilindedir. Bu tür yazılımlar elde ettikleri ayrıcalıklı yetkiler ile sistemde yaptıkları işlemleri, siber güvenlik uygulamaları ve örneğin anti-malware/virüs programları taramaları karşısında ‘’meşru‘’ gösterebilirler. Bu şekilde sistemde yapılan bir değişiklik, siber güvenlik taramalarında sanki yetkili kullanıcı tarafından yapılmış gibi görüneceğinden, taramalar bir uyarı vermeyebilir.[174]

Rootkitler yönetici izinleri sayesinde diğer malware tiplerinin özelliklerinden farklı olarak, onların yapamadığı pek çok işlemi gerçekleştirebilirler. Bu tür yazılımlar sistemdeki izlerini silebileceği gibi sistemdeki farklı verileri de silebilirler. Yine rootkitler kendilerini gizledikleri gibi sisteme sızdırılmış diğer malware yazılımları da gizleyebilirler. Dosya isimlerini değiştirebilirler veya hackerın bağlanması için bazı portları açabilirler.[175] Örneğin bir USB bellek hediye edildiğinde, bu belleğin içinde kullanıcının göremediği ve tarama yazılımları tarafından da algılanamayan bir rootkit mevcut ise bu sayede rootkit evvela bağlandığı sisteme geçecektir. Daha sonra bu sistemde de aynı şekilde yönetici izinleri elde ederek kendini gizleyecek, arka kapılar

[173] Kaspersky, *What Is Rootkit- Definition and Explanation*, https://www.kaspersky.com/resource-center/definitions/what-is-rootkit, (ET: 02.03.2022).
[174] Kaspersky, *What Is Rootkit- Definition and Explanation.*
[175] Wikipedia, Rootkit, https://en.wikipedia.org/wiki/Rootkit#cite_note-2, (ET: 03.03.2022) / Refik SAMET ve Ömer ASLAN 2018, age. s. 230, 231; Türkay HENKOĞLU 2014, age. s. 87.

oluşturacak veya sair işlemler gerçekleştirerek hackerın sisteme sair zararlı yazılımlar yüklemesine ve çeşitli işlemler gerçekleştirmesine olanak sağlayacaktır. En önemlisi de rootkit hem kendisini hem de yapılan sair işlemleri olağan siber güvenlik önlemlerinden gizleyebilecektir. Lakin şüphesiz ki rootkitlerin tespiti ve temizlenmesine dair yazılımlar ve bir kısım üst seviye tarama-algılama yöntemleri de mevcuttur.[176]

2.2.2.4.3.2. Ransomware

Ransomware temel olarak, yerleştirildiği sistemdeki dosyaları kriptolayan veya sair şekillerde dosyaya erişimi engelleyen ve kriptonun çözülmesi için hackerların fidye talep ettiği yazılımlardır. İsimlendirilmelerinde fidye istenmesi durumu baskın çıkmış ise de bu yazılımların esas özelliği dosyaları veya sistemlerdeki farklı unsurları gerçek yetkililerin erişimine engellemesidir. Kriptolama veya sair şekilde yapılan engelleme sistemdeki tek bir dosyaya, dosya içindeki verilere veya sistemdeki bir çok dosyaya yönelik gerçekleştirilebilir. İşletim sistemlerinin ve ağdaki farklı noktala erişimin de ramsomware kullanılarak engellenmesi mümkündür.[177] Ransomware sistemdeki kriptolama ve engellemeleri gerçekleştirdikten sonra, hackerlar bir şekilde sistem kullanıcısı ile iletişime geçer ve kripto para[178] vb. bedeller karşılığı kriptoyu/engeli aşacak anahtarları/yöntemleri bildireceklerini beyan ederler.[179] Bu tip yazılımlar, tipik özelliklerine ek olarak fidye verilmediğinde sistemi ya da dosyayı tamamen bozacak/silecek türde virüs özellikleri de gösterebilir. Bu sebeple fidye verilmediğinde kriptonun çözülememesine ek olarak sistemlerde ciddi zararlar da meydana gelebilmektedir.[180]

Türkiye, ransomware saldırıları yönünden dünyada ilk sıralarda yer almaktadır.[181] Her türlü malware gibi ransomware özelliğine sahip yazılımlar da çok çeşitli yollarla sistemlere enjekte edilebilirler. Bu sebeple bir web sitesine ya da spam maile gömülü bir ransomware'in ya da trojan niteliğindeki masum görünen bir

---

[176] Kaspersky, *What Is Rootkit- Definition and Explanation.*
[177] Olgun DEĞİRMENCİ (2019), ''Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi'', *Yaşar Hukuk Dergisi*, C. 1, S. 2, ss. 175-204, s. 178, 179 vd.; FBI, Ransomware, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware, (ET: 02.03.2022); Şeref SAĞIROĞLU 2018, age. s. 27, 28, 29.
[178] EUROPOL (2020), *Internet Organised Crime Threat Assesment*, s. 17.
[179] The NATO Cooperative Cyber Defence Centre of Excellence (2021), *Recent Cyber Events no: 12*, https://ccdcoe.org/uploads/2021/09/Report_The_Global_Threat_A4-1.pdf, (ET: 03.03.2022), s. 2.
[180] A. Nurdan SARAN 2019, age. s. 227.
[181] https://www.bthaber.com/turkiye-en-cok-fidye-yazilimi-saldirisi-alan-ulkeler-arasinda-ilk-5te/, (ET: 03.03.2022).

ransomware'in herhangi biri tarafından bilgisayarına indirilmesi mümkündür. Önemli ransomware saldırıları ise genellikle yüklü miktarda fidye ödeyebilecek kişilerin sistemlerine ve/veya fidye ödemeye değer verileri barındıran sistemlere, daha çok da şirketlere yönelik gerçekleştirilmektedir. Bu tür saldırıların arkasındaki örgütleri bulabilmek çok da kolay değildir. Örneğin ransomware kullanarak 70 milyon Euro fidye talep eden hackerlar, Fransız Ulusal Jandarması, Ukrayna Ulusal Polisi, FBI, INTERPOL ve EUROPOL'ün ortak çalışmaları sonucu ancak tespit edilebilmiş ve yakalanabilmiştir.[182]

2.2.2.4.3.3. Spyware

Spyware, bir casusun gerçek dünyada yaptığı tüm takipleri siber uzayda hedef sisteme yönelik yapmak adına geliştirilmiş yazılımlardır. Bu tip yazılımlar trojan özelliği göstererek sıradan bir hava durumu ya da müzik uygulaması görünümüyle uygulama marketlerde sunuluyor olabileceği gibi trojan özelliği göstermeyen ve mağdurların istemeden maruz kaldıkları/zorla-gizlice sistemlere sızdırılan versiyonları da mevcuttur.[183] Spyware hedef sistem ile hacker arasında bir köprü oluşturarak, ağ bağlantısı üzerinden hedef sistemde gerçekleşen neredeyse tüm faaliyetleri hackera bildirebileceği gibi sistemdeki belirli noktaları aktif hale getirerek ortam dinlemesine de imkan sağlayabilir. Örneğin spyware kullanılarak mikrofona erişilmesi suretiyle dinleme, kameraya erişilmesi suretiyle izleme, konum verileri üzerinden takip, arama ve mesaj geçmişi ile trafik bilgileri gibi sair her türlü veriye erişim gerçekleştirilebilir. Bunlardan ransomware ve/veya rootkit tipi yazılımlar ile benzer özelliklere sahip olanları çeşitli verilere erişimi engelleyebileceği gibi bir kısım işlemler gerçekleştirdikten sonra bu işlemlere dair geçmişi de silebilir. Bu tür bir spyware, verileri sızdırdığı sunucu ile arasındaki ağ trafiğinin kayıtlarını silebilir ve bu sayede fark edilmesini geciktirebilir.[184]

En ünlü spyware tipi, NATO raporlarında da bir tehdit unsuru olarak geçen İsrail yapımı Pegasus'tur. NSO firmasının geliştirdiği bu spyware'in hedefi; özellikle politikacılar, gazeteciler, sivil toplum kuruluşu liderleri gibi toplumun önde gelenleri

[182] https://www.interpol.int/en/News-and-Events/News/2021/Ransomware-gang-arrested-in-Ukraine, (ET: 03.03.2022),
[183] Pegasus'a dair aynı yönde açıklamalar için bkz. The NATO Cooperative Cyber Defence Centre of Excellence, *Recent Cyber Events no: 12*, s. 2.
[184] USOM (2014a), *Akıllı Telefonlarda Güvenlik*, s. 14, 15; The NATO Cooperative Cyber Defence Centre of Excellence, *Recent Cyber Events no: 12*, s. 3.

ve izlenmesi ya da şantaj yapılabilmesi görece önemli kişiler olmuştur. Yine baskıcı rejimlerin muhalifleri izlemek ve dinlemek adına bu yazılıma başvurduğu da belirtilmektedir.[185]

Veri trafiğinin kriptolanması ve örneğin Whatsapp mesaj ya da VoIP iletişiminin uçtan uca şifrelenmesi, man in the middle/sniffing atakları için geçerli bir önlemdir. Fakat iletişimin tarafı olan sistem içine yüklü bir spyware, normal kullanıcı gibi sohbet kayıtlarını görebilir ve eğer bu yönde bir özelliğe sahipse telefonu dinleyebilir. Pegasus ise bu tür sıradan özelliklerinden değil, başarılı biçimde casusluğu yapabilmesi, sistemde fark edilmemesi, nasıl bulaştığı üzerine muammaların bulunması ve özellikle de devlet başkanları gibi yüksek koruma altındaki kişilerin sistemlerine dahi sızdırılabilmesinden dolayı bu derece ünlüdür. Ayrıca Pegasus'un Whatsapp VoIP aramaları üzerinden yapılan veri gönderimi sırasında bulaşabildiği yönünde haberler çıkması,[186] devletlerin ve istihbarat örgütlerinin fark ettirmeden sistemlere bu yazılımı sızdırdığı ya da NSO'nun bu yazılımı çeşitli devletlere/istihbarat örgütlerine sattığı gibi iddialar da Pegasus'u korkulan ve ünlü bir spyware yapmıştır.[187]

2.2.2.4.3.4. Virüs

Bir sisteme yüklendiğinde diğer dosyalara da kodlarını enjekte eden ve onları da virüslü veri dosyası haline getiren virüs özellikli yazılımların temel amacı, bu şekilde mümkün olduğunca fazla sisteme ve veri dosyasına bulaşmak, nihayetinde de bulaştığı alanlara zarar vermektir.[188] Bu yönüyle virüslerin worm/solucanlardan farkı, solucanların çoğalmak için başka bir dosyaya ihtiyaç duymamaları ve kendilerini kopyalamalarıdır.[189] Bu sebeple eğer bir yazılım aynı zarar verici özellikleri gösteriyor fakat kendini kopyalayamıyor ise virüs, kopyalayabiliyor ise worm olarak adlandırılır.

---

[185] The NATO Cooperative Cyber Defence Centre of Excellence, *Recent Cyber Events no: 12*, s. 2.
[186] Financial Times, *WhatsAPP Voice Calls Used To İnject Israeli Spyware On Phones*, https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab, (ET: 02.03.2022).
[187] New York Times, *F.B.I. Secretly Bought Israeli Spyware and Explored Hacking U.S. Phones*, https://www.nytimes.com/2022/01/28/world/middleeast/israel-pegasus-spyware.html, ET: 03.03.2022; Aljazeera, India bought Israeli Pegasus spyware as part of weapons deal: NYT, https://www.aljazeera.com/news/2022/1/29/india-bought-israeli-pegasus-spyware-as-part-of-weapon-deal-nyt, (ET: 03.03.2022); BBC, Pegasus: Spyware Sold to Government's Targets Activist's, https://www.bbc.com/news/technology-57881364, (ET: 03.03.2022).
[188] Refik SAMET ve Ömer ASLAN 2018, age. s. 228; Suraj GANGWAR ve Vinayak NARANG 2020, age. s. 25.
[189] Türkay HENKOĞLU 2014, age. s. 187, 188, 189.

Fidye yazılımı gibi maddi bir çıkar amacıyla kullanılması mantıklı olmayan virüsler, özelliklerinden dolayı salt zarar verme saikiyle kullanılan yazılımlardır. Günümüzde bir milyondan fazla virüs çeşidi olduğu belirtilmektedir.[190]

2.2.2.4.3.5. Trojan

Bir malware eğer faydalı veya en azından zararsız bir yazılım gibi görünüyor, bu sebeple görünürde hackerın esas niyetini belli etmeyecek bir izlenim veriyor fakat özünde kötü amaçlar barındırıyor ise bu yazılımların sahip olduğu aldatıcı özellik, onlara Truva Atı benzetmesi sebebiyle ‘’trojan‘’ denilmesini sağlamıştır.[191] Trojan özelliği gösteren yazılımların bu aldatıcılıkları dışında başka hiçbir spesifik özelliği yoktur. Bunlar üretim durumlarına göre rootkit, virüs, spyware ve sair malware tiplerinin özelliklerine sahip fakat aldatıcı bir görünüm sergileyen yazılımlardır.

USOM, raporlarında önemli bir hususa dikkat çekmektedir. Bu husus, herhangi bir sistem ya da uygulama yazılımının belirli sabit ayarlarla sistemlerin üretim aşamalarında yerleştirildiği ve bu sayede kullanıcının onayı alınmaksızın sistemin belirli verilerinin tıpkı bir spyware gibi üçüncü taraflara aktarılabildiğidir.[192] Bu tür yazılımlar tipik trojan kavramının içine dahil olmasa da özünde yaptıkları işlev benzerdir. Yalnızca burada kullanıcı verileri hizmetin geliştirilmesi amacıyla yani müspet bir gaye uğrunda ve toplum bu konuda bilgilendirilerek elde edilir. Yine bir kısım uygulama yazılımı ve özellikle mobil uygulamalar, kullanıcıdan izin alarak çeşitli verilere erişim yetkisi almakta ve genellikle okunmayan ve hatta onay/ret butonu da olmayan tek tip sözleşmelerde bu erişimlerin ve aktarılan verilerin ne şekilde kullanılacağı bilgisi topluma/kullanıcıya verilebilmektedir.[193] Bu tip uygulamalardan bazıları hiç gerekmediği halde kameraya, rehbere ya da galeriye erişim izni almadan çalıştırılamasa ve bu da açıkça menfi bir amacı göstermekte olsa da bunlar tipik trojan kavramına dahil değildir.[194]

Tipik trojanlar ya hiç izin almadan belirli yetkileri ve verileri elde ederler ya da izin alarak aldığı yetkileri-verileri suistimal ederek, amaç dışında kullanırlar. Örneğin bir şarkı dinleme uygulaması görünürde son derece güven verdiği için indirilmiş

[190] Cebrail TAŞKIN 2018, age. s. 315.
[191] Semih Töner ŞEN 2021, age. s. 127; Hamza ELBAHADIR 2021, age. s. 109; Şeref SAĞIROĞLU 2018, age. s. 31.
[192] USOM 2014a, age. s. 8, 9.
[193] USOM 2014a, age. s. 10. Age. s.10
[194] USOM 2014a, age. s. 12. Age. s.12

olabilir. Olması gerektiği şekliyle yalnızca hoparlör ve sair donanım ile bağlantı izni alan yazılım, çalıştırıldığı an sistemde beklenmedik sonuçlar doğuruyor ise burada tipik bir trojan söz konusu olacaktır. Bu beklenmedik sonuçlar apaçık görünür olabilir ve örneğin yazılım yüklendiği an kaybolur, programlar arasında bulunamadığı için silinemez ve fakat arka planda zararlı işlemlerini sürdürmeye başlar. Yine ransomware özelliği gösteren bir trojan çalıştırıldığı an dosyaları kriptolayabilir. Başka bir ihtimalde ise yazılım çalıştırıldığında sisteme zarar verebilir. Trojanın faaliyetlerinin gizli gerçekleşmesi ve kullanıcının saldırı gerçekleşirken yazılımı her şeyden habersiz biçimde kullanmaya devam ediyor olması da trajik bir ihtimaldir. Böyle bir durumda yazılım sohbet mesajlarına erişebilir, sistemdeki verilerde değişiklik yapabilir, internet üzerinden çeşitli bağlantılara veri gönderebilir ve hatta kullanıcı farkına varmadan sistemi vasıtasıyla suç bile işlenebilir. Örneğin namaz saati gibi masum uygulamaların kullanıcılardan habersizce terörist faaliyetlerde kullanılmış olan ByLock sunucularına bağlantı sağlamış olması, ‘’morbeyin‘’ olarak adlandırılan bu menfi olayın[195] tipik bir trojan kullanımı olduğunu göstermektedir.

2.2.2.4.3.6. Worm

Worm/solucan, enjekte olduğu sistemde kendi kendini çoğaltabilen zararlı yazılımları niteleyen bir kavramdır. Worm kendisini kopyalayarak yayılabildiği için diğer veri dosyalarına bulaşması gerekmez. Bu sebeple ağdaki tek bir sistem üzerinden tüm ağa, ağ üzerinden diğer ağlar ile yapılan iletişimler sonucu diğer ağlardaki sistemlere ve bu şekilde çok büyük çaplı bir coğrafyaya yayılabilir.[196]

2.2.2.4.3.7. Keyloggler

Bulunduğu sistemdeki ekranı ya da fare-klavye-tuş takımını gözleyebilen özellikteki zararlı yazılımlara genel olarak keylogger denilmektedir. Bu tür yazılımlar bu gözlemlerini yalnızca sistemdeki bir noktada depolayabilecekleri gibi diğer malware tiplerinin özelliklerine de sahip ise sistemde açık kapılar oluşturabilir ve

---

[195] Habertürk, Mor Beyin Nedir, https://www.haberturk.com/mor-beyin-nedir-mor-beyin-yazilimi-nedir-1772655, (ET: 02.03.2022).

[196] Semih Töner ŞEN 2021, age. s. 127; Suraj GANGWAR ve Vinayak NARANG 2020, age. s. 25; Burak ÇEKİÇ (2006), *İnternet Aracılığı ile İşlenen Suçlar,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Yüksek Lisans Tezi, İstanbul, s. 71, 72; ‘’*Sıradan bilgisayar virüsleri, sisteme girdikleri zaman sistem dosyalarını etkileyerek, kendilerini bilgisayarın kritik bir noktasına kopyalarlar ve aktif olabilmek için kullanıcılara ihtiyaç duyarlar. Ancak worm'lar kopyalanmak için taşıyıcı program veya dosyalara ihtiyaç duymazlar*.‘’ Hamza ELBAHADIR 2021, age. s. 25.

hackerın bağlatı ile bu dosyalara erişmesini sağlayabilirler. Yine keylogger sistemdeki belirli yetkileri edinerek bu dosyaları ağ üzerinden hackera gönderebilir veya hackerın anlık olarak bu gözlemleri yapmasını sağlayabilir.[197]

Bulunduğu sistemdeki ekranı ya da fare-klavye-tuş takımını gözleyebilen yazılımlar eğer daha kapsamlı casusluk faaliyeti gerçekleştirebiliyor ise bunlar spyware olarak adlandırılacaktır. Yine kendini aldatıcı biçimde faydalı ya da zararsız bir yazılım olarak gösteren keylogglerlar, literatürde genellikle trojan olarak adlandırılmaktadır. Bu sebeple bilinmesi gerekir ki tek özelliği klavye hareketlerini kaydetmek olan bir yazılım da hackingde kullanılabilmekte ise de keylogger kavramı aynı zamanda bir yazılımın ekranı ya da fare-klavye-tuş takımını gözleyebilme özelliklerine vurgu yapılmak istendiği zaman da kullanılır.

Keylogglerlar yönünden tipik bazı örnekler vermek, konunun daha iyi anlaşılmasına yardımcı olacaktır. Örneğin hacker brute force saldırısı sonucu uzaktan şifreyi kırarak sisteme bağlanır, bir rootkit yükler ve ardından da keylogger yükler. Rootkit hem kendini gizler hem keylogger'ı gizler ve hem de keylogger'ın sistemden hackera veri gönderebilmesi için arka kapıları oluşturur. Bir diğer tipik örnekte ise kişi para ödememek için internetten bedelsiz oyun indirir, oyunun kurulum dosyaları içerisinde bir keylogger bulunabilir. Başka bir örnekte ise kişi Whatsapp'a alternatif bir sohbet uygulaması yükler, bu uygulama klavyeye erişim izni alır ve verilerin uygulamanın sunucularında barındırılmasının haricinde uygulama, cihazdaki tüm klavye hareketlerini üçüncü taraf sunuculara gönderebilir.

2.3. YETKİSİZ ERİŞİM VE ARAYA GİRME SUÇLARI İLE İLİŞKİLİ HACKİNG YÖNTEMLERİ

Bir hacking operasyonu gerçekleştirilirken, genellikle pek çok saldırı birlikte gerçekleştirilir ve bu da birden fazla suçun tipikliği içerisinde kalan hareket ve neticenin meydana gelmesine sebep olur. Nihai saldırıya yönelik öncül saldırılar da gerçekleştirilebilir ve örneğin amacı hedef sistemleri bozmak olan bir DDoS saldırısı için öncelikle botnet ağı oluşturmaya yönelik saldırılar gerçekleştirilir ve sistemlere yetkisiz erişim olanağı elde edilir.

---

[197] Hamza ELBAHADIR 2021, age. s. 109; Gunter OLLMANN (2007), *The Phishing Guide Understanding & Preventing Phishing Attacks*, s. 37; Çığır İLBAŞ (2009), *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi*, Başkent Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, s. 29.

Aşağıda açıklanan hacking yöntemlerinin her birinin nihai hedefi sisteme yetkisiz olarak erişmek ve/veya araya girerek veri trafiği izlemek değildir. Ancak bu hacking operasyonları sırasında üçüncü taraf sistemlere yönelik TCK md. 243'e konu olan yahut yakından ilişkili fiiller gerçekleştirildiğinden, tipik olarak TCK md. 243'teki suçlar ile anılmayan hacking yöntemleri de aşağıda açıklanmıştır. İkinci olarak, nihai amacı hedef sisteme yetkisiz olarak erişmek ve/veya araya girerek veri trafiği izlemek olan, neticede de TCK md. 243'teki suçların oluştuğu tipik hacking yöntemleri de aşağıda açıklanmıştır. Kimi hacking yöntemleri ise bu suçlardan her ikisine dair fiilleri de bünyesinde barındırmaktadır. Bu sebeple bu alt başlıkta ''ilişkili'' kelimesi kullanılmıştır. Hacking olaylarının TCK md. 243'teki suçlar ile bağlantısının geniş biçimde açıklanması, konunun derinlemesine anlaşılabilmesi yönünde de fayda sağlayacaktır.

2.3.1. Yetkisiz Erişim Suçu ile İlişkili Hacking Yöntemleri

2.3.1.1. Genel Bilgiler

Bilişim sistemine yetkisiz olarak erişmek, çoğu durumda şu şekilde gerçekleşir: İlk olarak kablolu bağlantı portları veya kablosuz bağlantı noktalarına doğrudan ya da yetkili erişim için gerekli şifre-hard token vb. vasıta kullanılarak bağlanılabilir. İkinci olarak internet(*WAN*) ya da intranet(*LAN-CAN vb.*) ağ yapılarında, verileri barındıran sunuculara yine şifre ve sair gerekli unsur girilerek uzaktan bağlanılabilir. Bu iki neticeyi gerçekleştirebilmek için Firewall uygulamalarının yanıltılması amacıyla spoofing atakları yapılabilir ve/veya şifre ve sair bilgiyi elde edebilmek için phishing, brute force ve benzeri saldırılara girişilebilir. Yukarıda sayılanlar haricinde enjeksiyon saldırıları vasıtasıyla da yetkisiz erişim gerçekleşebilmekte ya da sisteme erişmeyi sağlayacak şifre ve benzeri bilgiler elde edilebilmektedir. Bu sebeple aşağıda şifrelerin elde edilebilmesi ve güvenlik uygulamalarının yanıltılabilmesi için kullanılan hacking yöntemleri de zikredilmiştir.

Yetkisiz erişim durumlarında hackingin amacı evvela sistemdeki verileri elde etmek olabilir. Veri sızıntıları günümüzde öyle büyük bir pazar oluşturmuştur ki EUROPOL'ün operasyonlar sonucu yaptığı tespitlere göre milyonlarca kişinin sızdırılmış ve çalınmış verilerini kayıt altında tutan örgütler bulunmakta, örgütler verileri dark web'de ya da sair ortamlarda satmaktadırlar.[198] İkinci olarak sistemi

[198] EUROPOL, Internet Organised Crime Threat Assesment, s. 16.

bozmak ya da içeriğinde değişiklikler yapmak veya botnet ağında olduğu gibi sistem vasıtasıyla bir kısım eylemlerde bulunmak amacıyla yetkisiz erişimler gerçekleştirilebilir. Bu sebeple aşağıda sisteme yetkisiz olarak erişildikten sonra gerçekleştirilen hacking yöntemleri yönünden de örnekler verilmiştir.

2.3.1.2. Brute Force

Brute force saldırıları, manuel olarak veya veri tabanındaki verileri otomatik olarak deneyen yazılımlar kullanılarak, yetkili erişim için şifre ve benzeri bir doğrulama girdisi isteyen sistemlere yetkisiz olarak erişmek için yapılır. Örneğin şifre ve kullanıcı adı girildiğinde bu bilgi önce uygulama sunucularına, oradan da bu verileri barındıran veri tabanı sunucusuna gönderilir ve girdiler ile veri tabanındaki bilginin eşleşmesi, sisteme erişim için şart koşulur. Deneme yanılma yöntemi olan brute force saldırıları sonucu eğer bu deneme tutarsa, saldırgan yetkisiz olarak sisteme erişebilecektir.[199]

Brute force saldırılarının başarılı olamaması için karşıdaki istemcinin bot olup olmadığını tespit etmeye, aynı IP üzerinden sınırlı sayıda deneme yapılabilmesine ve sair pek çok önleme dair siber güvenlik çözümleri mevcuttur. Ancak brute force saldırılarının tüm bunları aşması ve parolalar ne kadar kuvvetli olursa olsun tespiti mümkün olduğundan, bu saldırılara karşı çok aşamalı yetki kontrolünün mevcut olması gerekir. Bu sebeple şifrelerin yanında SMS/mail'e gönderilen kodun girilmesi, güvenlik soruları ya da hard token veya e-imza kullanımı tercih edilir. Eğer bu önlemler de aşılarak sisteme erişildikten sonra verilerin öğrenilmesinin önüne geçilmek isteniyorsa, kriptografik çözümler kullanılması gerekecektir. Sisteme erişim şifrelendikten ve/veya hard token kullanıldıktan sonra kasa oluşturma ve sair şekillerde verilere ulaşımın da şifrelenmesi ve nihayetinde de hash+salting uygulamalarıyla verilerin içeriğinin de kriptolanması bu yönde ciddi bir önlem olacaktır.[200]

Brute force saldırıları herhangi bir sisteme erişilirken ve örneğin manuel olarak açılan bir bilgisayara kullanıcı girişi yapabilmek ya da şifre isteyen bir ağ bağlantısına

[199] Onur AKTAŞ 2020, age. s. 116, 117, 118 vd.; Bünyamin DEMİR 2020, age. s. 115, 116, 117 vd.; Erhan SAYGILI 2018, age. 174, 175 vd.; Mustafa Yasir ŞENTÜRK 2018, age. s. 65, 66.

[200] Mevzuatımızda verilerin ve veri trafiğinin kriptolanması ile kriptoyu çözecek anahtarların ne şekilde saklanması gerektiği, siber güvenlik için bunlar yetmeyeceği için firewall-IDS-IPS ve sair güvenlik uygulamalarının ne şekilde çalıştırılması gerektiğine dair en ayrıntılı hükümler Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te mevcuttur.

dahil olmak amacıyla da yapılabilir. Örneğin doğrudan bir SSID'ye[201] brute force saldırısı yapılabilir ve bu şekilde şifre kırılarak wi-fi ağına dahil olunabilir. Bu aşamadan sonra da çok çeşitli saldırılar ağda gerçekleştirilebilir. Lakin genellikte brute force saldırıları web ya da intranet sunuculara uzaktan bağlanmada kullanılır. Günümüzde veriler çok değerli olduğundan, bir güvenlik görevlisinin sosyal medya hesabının şifresinin kırılması bile sohbet geçmişinden yola çıkılarak ciddi bir banka soygununa zemin hazırlayabilir. ABD başkanlık seçimlerinin bile veri tabanlarına yapılan sızmalar sonucu elde edilen bilgiler dolayısıyla manipüle edildiği iddiaları mevcutken,[202] brute force saldırıları yetkisiz erişimler için önemli bir basamak durumundadır.

2.3.1.3. DoS-DDoS

DoS ve DDoS saldırılarının temel amacı, hedef sistemin işleyişini aksatmak, yavaşlatmak veya sistemde kalıcı hasarlara sebep olmaktır. Saldırı bu temel amaçla sınırlı kalabileceği gibi düzgün işlemeyen sistemlerden istifade ederek yeni saldırılar da gerçekleştirilebilmektedir. Bu saldırılarda hedef sistemin istemci trafiğini karşılayabilme kapasitesi(*hafıza-bant genişliği*) veya istemci trafiğini algılayabilme yeteneği, saldırgan sistemlerden gönderilen veri paketleri vasıtasıyla bozulur. Kapasiteyi zorlayan veri paketleri şüphesiz ki sayısal fazlalığa veya büyüklüğe, yeteneği zorlayanlar ise paketlerin hedef sistemler tarafından algılanamayacak biçimde gönderilmesine bağlıdır.[203]

DoS ile DDoS arasındaki ayrım önemlidir. DDoS saldırısı evvela botnet ağı yani ele geçirilmiş zombi/köle sistemler üzerinden ve bu köle sistemler yönünden cebren gerçekleşir. İkinci olarak botnet ağı teşkil etmeyen birden fazla sistemi yöneten tek bir hackerın saldırısı mevcut olabileceği gibi hacktivist eylemlerde olduğu gibi binlerce internet kullanıcısı kendi istekleriyle sistemleri üzerinden DDoS saldırısı da başlatabilir. DoS saldırısında ise tek bir sistem kullanılarak saldırı gerçekleştirilir.[204]

---

[201] Kablosuz ağ bağlantı noktasının bağlantı isteğinin gönderildiği/şifre isteyen unsuru SSID olarak isimlendirilir.

[202] Bu iddialara dair detaylı anlatım için bkz. Ali Burak DARICILI (2017), ''Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi'', *ULİSA: Uluslararası Çalışmalar Dergisi Özel Sayısı,* C. 1, S. 1, ss. 1-24, s. 16, 17, 18 vd.

[203] USOM (2014b), DDOS El Kitabı, s. 3.; Hamza ELBAHADIR 2021, age. s. 117, 118 vd.; Semih Töner ŞEN 2021, age. s. 125; Şeref SAĞIROĞLU 2018, age. s. 31.

[204] Semih Töner ŞEN 2021, age. s. 125; Hamza ELBAHADIR 2021, age. s. 123 / DoS'un tek istemci, DDoS'un ise etkileşimli çok sayıda istemciden (*köle veya değil*) yapılan sömürme talepleri olduğu yönünde bkz. Cemal ARAALAN 2021, age. s. 102, 103; Serkan BÜYÜKÇAĞLAR 2013, age. s. 79.

Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nde DoS, DDoS ve köle bilgisayarın normatif tanımları yer almaktadır. Yönetmelik md. 3/1'de DoS ''*hizmet dışı bırakma*'', DDoS, ''*dağıtık hizmet dışı bırakma*'', köle bilgisayar ise ''*herhangi bir amaçla kullanılmak üzere, zararlı yazılımlar veya kötü niyetli kişiler tarafından uzaktan yönetilen internete bağlı bilgisayar*'' şeklinde tanımlanmıştır. Yargıtay Ceza Genel Kurulu'nun 2016/544 E. 2020/127 K. sayılı içtihadında ise DDoS saldırılarına dair detaylı açıklamalar yer almıştır:

> ''*Asayiş Şube Müdürlüğü, Ar-Ge ve Bilgi İşlem Büro Amirliği, İnternet ve Bilişim Suçları Kısmına getirildiğinin, açılımı "Distributed Denial of Service" olan ve "Dağıtılmış Servis Sömürüsü" anlamına gelen DDoS saldırılarının yapılış şeklinin bir saldırganın daha önceden tasarladığı veya hack yolu ile hazırladığı birçok makine (3. şahıslara ait bilgisayarlara yüklenmiş trojanlar) üzerinden bilgisayara veya hosta saldırı yapmak suretiyle hedef sistemin trafiğini arttırarak işlemez hâle gelmesini amaçlayan bir saldırı çeşidi olduğunun, kısaca bu saldırı şeklinin bilişim sistemini engellemek, bozmak veya işlemez hâle getirmek için bilgisayar korsanları tarafından kullanıldığının, koordineli olarak yapılan bu işlemin hem saldırının boyutunu artırdığının hem de saldırıyı yapan kişinin gizlenmesini sağladığının, bu nedenle de saldırganı bulmanın zorlaştığının, çünkü saldırının merkezinde bulunan saldırganın aslında saldırıya katılmadığının, sadece daha önceden etkisi altına aldığı bilgisayarları kullanarak yönlendirme yoluyla saldırı yaptığının, saldırının tek IP adresinden yapılması hâlinde Firewall denilen bir çeşit güvenlik sistemi tarafından bu saldırının rahatlıkla engelleyebileceğinin, ancak DDos ataklarında olduğu gibi çok sayıdaki IP adresinden yapılan saldırıların Firewall'un devre dışı kalmasını sağladığının, bu özelliğin onu DoS saldırısından ayırdığının …*''[205]

Bilinmesi gerekir ki DoS/DDoS atakları yalnızca web sunuculara yapılmaz. Örneğin kablosuz ağa dahil olmak isteyen sistemlerin ağ erişim noktasına erişememesi ve/veya bağlantının kopması için bunu sağlayacak veri paketleri bağlantı noktasına iletilebilir ve bu sayede ağda iletişim aksatılabilir.[206] DNS sunucular da bu saldırıların hedefi olabilir ve DNS sunucuya gönderilen aşırı yoğun istekler ya da algılanamaz veri paketleri sayesinde DNS sunucular işlevlerini yerine getiremez hale getirilebilir.[207]

[205] Yargıtay CGK 2016/544 E. 2020/127 K.
[206] Besim ALTINOK 2021, age. s. 79, 80 vd. / Eğer hedef alınan sistem sunucu değil de ağdaki router ve sair bir sistem ise buna PDoS denilmektedir. Bu konuda bkz. Hamza ELBAHADIR 2021, age. s. 125.
[207] BİLGEM (2020), *Alan Adı (Domain) Sistem Yönetimi Rehberi*, s. 28, 29, 30, 31.

Çok büyük çaplı saldırılarda erişim sağlayıcı sistemlerinin bant genişliği doğrudan etkilenebileceğinden, bu saldırılardan dolaylı olarak omurga trafiğinin ve pek çok internet kullanıcısının etkilenmesi de mümkündür.[208]

Web sunucular haricindeki sistemlere yapılan saldırılara yönelik bir örnek, DHCP sunucular üzerinden verilebilir. İnternet erişiminde, yerel ağdaki sistemi internet/WAN'a çıkartan router/modem'in IP adresi ve yerel ağda da DHCP sunucunun ya da bu işlevi gören modemin dağıttığı NAT/iç IP adresleri bulunur. DHCP sunucular veya bu işlevi gerçekleştiren cihazlar, ağdaki her bir sisteme IP dağıtımı yaparken bunu her sistemin kimlik bilgisi olan MAC adreslerine göre yapar. Yerel ağda bu şekilde MAC-IP dağıtımı yapıldığında, atanabilecek IP adresleri sınırsız değildir. Eğer IP'lerin eşleşmesi gereken MAC adresleri statik olarak belirlenmemişse; ağdaki mevcut sistem sayısından çok daha fazla sistemin istemde bulunduğu izlenimi yaratılarak sürekli farklı MAC adreslerinden DHCP sunucuya iç IP atama isteği gelir ise bu durumda DHCP(*protokol*) düzgün çalışamayacaktır. Böyle olunca yerel ağdaki haberleşme de IP atanamadığı için durur ve DoS etkisi yaratılır.[209]

DoS/DDoS saldırıları, siber güvenlik bakımından küresel ölçekte oldukça fazla önemsenmektedir. Covid-19 sonrası yaşanan dijitalleşme akımının ise bu önemi artırdığı belirtilmektedir. Zira pek çok toplumsal hizmet dijitalleşmiş olup, bunların saldırılar sonucu aksatılmasıyla kamu düzeni ciddi biçimde bozulabilir.[210] Lakin DDoS geçmişte de oldukça yıkıcı sonuçlar doğurmuştur. Örneğin Estonya toplumuna karşı yapılan DDoS saldırıları sonucu ülkesel bir felaket yaşanmıştır. Aynı durum Rusya-Gürcistan savaşı sırasında Gürcistan aleyhine de gerçekleşmiştir.[211] Toplumsal olmasa da özellikle bankacılık sistemine yönelik ciddi DDoS saldırılarına örnek olarak, 2014 yılında açıklanan ve tarihin en büyük veri ihlallerinden biri olarak adlandırılan, JPMorgan başta olmak üzere bir çok finans kuruluşuna karşı gerçekleştirilen[212] DDoS saldırıları verilebilir.[213]

---

[208]Ahmet ÜNAL (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 Yüksek Lisans Tezi, İstanbul, s. 11, 12, 13, 14, 15, 16 vd.

[209] Gökhan USTA (2018), *Bilgisayar Ağlarında Saldırı ve Savunma*, Seçkin, Ankara, s. 91, 92, 98.

[210] Arturs LAVRENOVS (2021), ''Towards Remediating DDoS Attacks, The NATO Cooperative Cyber Defence Centre of Excellence'', İçinde, *ICCWS 2021*, ss. 152-158, Talinn,, Estonya, s. 152.

[211] Semih Töner ŞEN 2021, age. s. 143, 144, 145.

[212] Wikipedia, JP Morgan Chase Data Breach, en.wikipedia.org/wiki/2014_JPMorgan_Chase_data_breach, (ET: 02.03.2022).

[213] New York Times, JPMorgan and Other Banks Struck by Hacker, https://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html,

Ülkemizdeki sistemlere karşı ya da ülkemizden dışarıdaki hedeflere yönelik yapılan DDoS saldırılarına örnek olarak; Avusturya'ya Türk hackerlar tarafından yapılan saldırı,[214] Anonymous tarafından THY web sunucularına yönelik gerçekleştirilen ve maddi kayba neden olan saldırı[215] ve RedHack'in Polnet sunucularına karşı gerçekleştirdiği saldırı verilebilir.[216]

2.3.1.4. Botnet ve Köle Bilgisayar Kullanımı

Botnet ağları spam göndermek, malware enjeksiyonu, ziyaretçi sayısı manipülasyonu, kara propaganda gibi çok farklı amaçlar doğrultusunda kullanılabildiği gibi botnet'in en yaygın görünümü DDoS saldırılarında kullanılmasıdır. Botnet, hacker tarafından ele geçirilmiş bilişim sistemlerinin oluşturduğu köle sistemler ağıdır. Bu ağ IoT sistemlerin, akıllı telefonların ya da bilgisayarların yani çok farklı tipte sistemlerin oluşturduğu bir ağ olabilir.[217] Genellikle bu ağın oluşturulması için sistemlere bu ele geçirmeyi sağlayacak ve hacker'ın bağlanmasına imkan verecek malware yazılımlar enjekte edilir. Çoğu zaman bu yazılımlar trojan özelliği gösterdiği için kişiler fark etmeden sistemlerine bu yazılımları kurar ve botnet ağına kendileri katılırlar. Botnet ağında kullanılabilecek yazılımlardan bazıları rootkit özelliği göstererek root yetkisi alabileceği ve kendini gizleyebileceğinden, anti-malware taramalarında çıkmayabilmektedir.[218]

Normalde botnet başlığı altında açıklanmıyor olsa da işbu tezde her bir yöntem ayrı ayrı açıklanmadığından, ActiveX saldırılarının da en müsait alt başlık olan bu başlık altında açıklanması uygun olacaktır. Windows sistemlerde, yazılımların internet üzerinden güncellenmesi veya sair şekillerde bağlantı sağlayan karşı tarafça kullanılabilmesi için AciteX adı verilen yazılımlar bulunur. Bu sayede bir yazılım

(ET: 03.03.2022); CNBC, JPMorgan and Other Banks Struck By Cyberattack, https://www.cnbc.com/2014/08/27/fbi-probes-possible-hack-at-jpmorgan-report.html, (ET: 03.03.2022).

[214] Posta, Avusturya'ya saldıran Türk hacker bulundu' iddiası: 'General Osman' adıyla biliniyor http://www.posta.com.tr/avusturya-ya-saldiran-turk-hacker-bulundu-iddiasi-general-osman-adiyla-biliniyor-haberi-1272902, (ET: 02.03.2022).

[215] Serkan BÜYÜKÇAĞLAR 2013, age. s. 94.

[216] https://t24.com.tr/haber/emniyet-genel-mudurlugunun-sitesi-redhack-tarafindan-cokertildi,208778, (ET: 02.03.2022).

[217] Ersin MASUM ve Refik SAMET 2018, age. s. 114.

[218] Cemal ARAALAN 2021, age. s. 104 / Ersin MASUM ve Refik SAMET 2018, age. s. 113, 114; M. Zekeriya GÜNDÜZ (2013), *Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti,* Fırat Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Bilgisayar Eğitimi Anabilim Dalı Yüksek Lisans Tezi, Elazığ, s. 41; Ahmet ÜNAL 2014, age. s. 18; Refik SAMET ve Ömer ASLAN 2018, age. s. 227, 228, 229 vd.; Ersin MASUM ve Refik SAMET 2018, age. s. 114.

otomatik olarak internet üzerinden, güncelleme dosyaları gibi belirli dosyaları indirebilir veya işlemleri yapmak için internet üzerinden yönlendirilebilir. Eğer sistemdeki mevcut ActiveX yazılımların kullanımı hackerlar tarafından ele geçirilir ise sistem çok rahat biçimde köle bilgisayar olarak botnet ağına dahil edilebilir. Yine ActiveX kullanımına müsait bir yazılım hacker tarafından internet ağına sokulur ve kurban tarafından indirilir ise aynı sonuç yaratılacaktır. ActiveX kullanımı için sistem yetkilisinin onayı gerektiğinden, ActiveX'in onayını elde edebilmek için hackerlar sistemde zaten var olan malwareleri kullanabileceği gibi internet üzerinden belirli linklere gömülü kodlar ya da AcitiveX izni isteyen uyarılar yollayabilmektedirler.[219] Netice olarak ActiveX'in kontrolünün ele geçirilmesi, sisteme rootkit yüklenmesi ile eşdeğer olanakları sunabilir ve botnet ağı oluşturmada ideal bir yöntem olabilir.

DDoS saldırılarında botnet ağına dahil köle sistemlerin çeşitli sebeplerle internete bağı kesilebilmekte veya bunlar kapatılabilmektedir. Bu durum da botnetin gücünün düşmesi ve neticede de hedef sistemin tekrar sağlıklı biçimde işlemesine yani DDoS'un başarısının aksamasına sebep olabilmektedir.[220] Bu yüzden botnet kullanımı, süreklilik arz eden DDoS saldırılarında kuvvetle muhtemel kesin bir başarı elde edemeyecektir. Fakat botnet ağı kullanılarak yapılan ve süreklilik arz etmeyen saldırılardan kesin bir başarı elde edilebilmesi mümkündür. Bu noktada botnet ağı kullanımının önemli sonuçlarından bir diğeri öne çıkmaktadır ki bu sonuç, botnet ağının adli bilişimin işini zorlaştırıyor olmasıdır.[221] Normalde hacker TOR ya da Tails(*Linux*) sürümlerinde bulunan gömülü ayarları kullanarak trafiğini hem kriptolar hem de üçüncü taraf sunucular ağı üzerinden geçirir. Botnet kullanımı ise bu trafiğe diğer bir üçüncü taraf olarak köle bilgisayarı da ekleyecektir. Eğer köle bilgisayarda da bu işler VPN ya da Proxy üzerinden gerçekleştiriliyor ise trafiğe başka bağlantı noktaları da katılacak ve iş oldukça karmaşık bir boyut alabilecektir. Bu sebeple köle bilgisayar ve botnet kullanımı esasında aynı zamanda çoğu hacking yöntemi açısından uygulanabilecek ek bir güvenli liman durumundadır.

[219] Hamza ELBAHADIR 2021, age. s. 85, 86.
[220] Gökhan USTA 2019, age. s. 28.
[221] Meselenin DDoS atakları yönünden açıklanması konusunda bkz. Arturs LAVRENOVS 2021, age. s. 154.

2.3.1.5. Enjeksiyon Saldırıları

Bir http isteğinin, komut çalıştırma isteğinin, veri paketinin, kodun ya da bir veri dosyasının hedef sistemlere gönderilmesine ve/veya hedef sistemde çalıştırılmasına yönelik saldırılar farklı çatı kavramlar altında incelenebilmekle birlikte, bunlardan pek çoğu en temelde ‘’enjeksiyon saldırısı‘’ olarak nitelendirilebilir.[222] İşbu tez içerisinde de konunun basitleştirilmesi açısından, hedef sistemlere karşı yapılan enjeksiyonlar sonucu gerçekleşen hacking olaylarının tek bir başlık altında açıklanması ve başlığın da enjeksiyon saldırıları şeklinde isimlendirilmesi uygun görülmüştür.

Enjeksiyon saldırıları temelde ikiye ayrılabilir. Bunlardan birincisinde, programlama dillerinin ve hedef sistemlerde bu dillerin çalıştırılmasına yönelik zafiyetlerin kullanılması sonucunda hedef sistemdeki verilere erişilir ve/veya veriler eklenir/değiştirilir/silinir. Bu tür enjeksiyon saldırılarından en temel olanı, SQL dilinin kullanıldığı SQL enjeksiyon saldırısıdır. İkinci olarak hedef sisteme bir kod ya da doğrudan veri dosyası gönderilerek/işlenerek, bunların hedef sistemde çalıştırılmasına yönelik enjeksiyon saldırıları mevcuttur ki bunlardan da en temel olanı XSS tipi saldırılardır.

Web’de istemci-sunucu arasındaki iletişimde istemci tarafın gönderdiği verilerde olmaması gereken girdiler kullanılarak, enjeksiyon saldırıları yapılabilir. Örneğin istemciden gelen ‘’bilgi edinme‘’ veya ‘’bilgi verme‘’ isteğine/sorgusuna cevap verecek sunucunun, hangi bilgileri istemciye göndermesi ve hangi bilgileri kabul etmesi gerektiğine yönelik SQL dili kullanılır. İnternet kullanıcıları bu dile müdahale etmez, örneğin bir butona tıklar ya da bir yazı yazar ve otomatik olarak sistem bunu SQL cümlecikleri ile değerlendirir ve algoritma işleyerek sunucudan veri gelir. Olması gereken bir web ortamında, sunucunun her türlü isteğe cevap vermemesi gerekir. Fakat eğer engellenmesi gerekirken engellenmemiş bir istek web ortamına iletilir ve sunucudan da veri dönüşü yapılırsa, nihayetinde olmaması gereken bir durum oluşur. İstenmeyen bu durumda, yetkisiz/şifresiz olarak sunucudan veriler çağrılabilir ve örneğin üyelerin kişisel verileri elde edilebilir ya da değiştirilebilir. Bu istenmeyen durum SQL dilinin işleyişi üzerinden gerçekleşmişse SQL enjeksiyon, diğer diller

[222] Benzer yönde bkz. Donald RAY ve Jay LIGATTI, *Defining Injection Attacks Technical Report*, University of South Florida Department of Computer Science and Engineering, https://cse.usf.edu/~ligatti/papers/bronies.pdf, (ET: 02.03.2022), s. 1, 2 vd.

kullanılmış ise NoSQL-OS enjeksiyon, SSI enjeksiyon gibi isimlendirmeler yapılır.[223] Aynı şekilde veri tabanında yapılan işlemlerde xml/xpath dili de kullanılıyor olabilir ve bu dil de çeşitli işaretler veya karşılığı bulunmayan harf kombinasyonları yahut kodlar ile manipüle edilerek erişim yetkisi olmayan bilgiler sunucudan çağırılabilir. Bu sayede yetkisiz olarak veri tabanlarındaki belirli içeriklere/sistemlere erişim sağlanabilir.[224]

Doğrudan site/uygulama içerisindeki girdiye açık ‘’*arama butonu vb.*‘’ bölümlere yapılan girdiler ile bu enjeksiyonlar yapılabileceği gibi tarayıcıdaki URL'ye girilen komutlar ile de veri tabanlarındaki zafiyetler üzerinden bu tür saldırılar gerçekleşebilir. Örneğin URL'ye girilen ve SQL dilini manipüle edecek türdeki bir SQL komutu ile yalnızca yetkili istemcilere iletilmesi gereken e-ticaret sitesi üyelerinin mail adreslerine dair veriler sunucudan çağırılabilir. Sistemi manipüle edebilecek pek çok SQL komutunu otomatik olarak giren hacking yazılımları da mevcut olduğundan, bu işler kısa sürede gerçekleştirilebilmektedir.[225]

Enjeksiyon saldırılarından farklı bir kavram olsa da kırılmış erişim kontrolünün de bu başlık altında açıklanması uygun olacaktır. Tıpkı SQL enjeksiyon saldırısında olduğu gibi belirli istekler yollanarak sunucu tarafta çalışan yazılımlar manipüle edilebilir ve yetkisiz olarak sistemdeki verilere erişilebilir. Doktrinde bu tür saldırılar için şu örnekleme yapılmaktadır:

> ‘’*Bu saldırı tipi için örnek olarak:http://example.com/user.php?u=user1 Yukarıda example.com sitesine user1 kullanıcısıyla girmiş ve user1 bilgilerini gören bir kullanıcı olsun, "u" parametresi eğer değiştirilirse yani http://example.com/user.php?u=user2 artık saldırgan kişi user1 olarak erişim yaptığı doğrulamayla user2 verilerini de görecektir. Bu şekilde yetkili başka bir kişinin yetkileriyle de istediği her şeyi yapabilecektir*.‘’[226]

Hedef sistemlere kodların ya da veri dosyalarının gönderildiği/işlendiği XSS ve benzeri tipteki enjeksiyon saldırılarında da temel zafiyet, hedef sistemlerin istemcilerden gelen girdileri/komutları düzgün şekilde filtrelemeden kabul etmesi ve bunlara göre işlem gerçekleştirmesidir. Bu sayede de hedef sistemde çalıştırılan

[223] Gökhan USTA 2019, age. s. 126, 127, 128; Hamza ELBAHADIR 2021, age. s. 143, 144, 145, 161 vd.; Bünyamin DEMİR 2020, age. s. 302, 303, 304 vd.; M. Alparslan AKYILDIZ ve Doğukan SANER (2020), *Web Sızma Testleri El Kitabı*, Gazi Kitabevi, Ankara, s. 73, 74 vd.
[224] Hamza ELBAHADIR 2021, age. s. 157, 158, 159; XML örneği için ayrıca bkz. Mustafa Yasir ŞENTÜRK 2018, age. s. 59.
[225] Onur AKTAŞ 2020, age. s. 285, 286, 287, 288, 289 vd.; Türk Standartları Enstitüsü, agb. s. 30.
[226] Mustafa Yasir ŞENTÜRK 2018, age. s. 59

yazılımlar manipüle edilebilmekte ve hackerın gönderdiği komut ya da kodlar çalıştırılarak istenmeyen durumlar yaratılabilmektedir. Bu tür kodlar hedef sistemlere veri dosyalarına ekli olarak gönderilip çalıştırılabileceği gibi tarayıcıya URL girilmesi gibi http isteklerine ve sair komutlara işli şekilde de gönderilebilir veya hedef bir web sitesi ise benzer yöntemlerle kaynak kodları değiştirilebilir. Örneğin bir sitede, www….xx=yyy şeklindeki bir URL'de ''xx'' girdisi yyy dosyasını çağırmakta ve istemci tarayıcısında görünmekte, xx girdisi ''haberler'' yyy de ''gündüz vakti hırsızlık'' dosya başlıklı bir haber olsun. Eğer XSS açığı varsa, tarayıcıya URL olarak Javascript ve sair kodları manipüle edecek şekilde ''yyy'' girdisi değiştirerek girilir ve sunucuya istekte bulunulursa, sunucu ''gündüz vakti hırsızlık'' dosyası yerine hackerın açıktan faydalanarak erişebildiği farklı bir veriyi çağırabileceği gibi hackerın ilettiği farklı bir veriyi de yayınlayabilir.[227]

Bu tür enjeksiyon saldırılarında hedef sistemlerin yanında hedef sistemlere bağlantı sağlayan üçüncü taraf internet kullanıcıları da hedef olabilirler. Örneğin hacker, hazırladığı zararlı kodları çeşitli yöntemlerle sunucuya iletir ve sunucudaki yazılımlarda bunları filtreleyen bir algoritma çalışmazsa, aynı internet ortamını kullanarak manipüle edilmiş sunucuya veri gönderenler de cevap olarak bu kodlar ile karşılaşabilirler. Mesela filtrelenmeden sunucu tarafa geçen yorumlarda, hacker yorum olarak tarayıcının otomatik olarak çalıştıracağı bir kod girmiş olabilir. Bu kod hedef sistemin işleyişini bozabileceği gibi sitenin diğer ziyaretçileri yoruma tıkladığı zaman onlara saldırı gerçekleştirecek şekilde de oluşturulabilir.[228] En belirgin örneği XSS saldırıları olan bu tip enjeksiyon saldırıları sonucunda hedef sistemlere enjekte edilen kodlar, bu hedef sistemlerde durum fark edilene kadar çalıştırılabilir. Örneğin XSS saldırısı gerçekleştirilmiş bir haber sitesini ziyaret edenler bir haberi okumak için tıkladıkları ve ilgili URL'ye eriştikleri zaman; sistemleri bu kodları otomatik olarak okuyup işlem gerçekleştireceğinden, tarayıcıda haber çıksa da arka planda kendisine gönderilen kodu okuyan istemci sistem, kullanıcısı farkında olmadan kodun gereğini yapabilir ve örneğin istemeden ilgili siteye üye olabilir, başka sitelere bağlantı gerçekleştirebilir, çeşitli cookieleri karşıya iletebilir, istemciyi saldırganın kontrolündeki başka bir sunucuya yönlendirebilir.[229]

[227] Onur AKTAŞ 2020, age. s. 185, 186 vd.
[228] Age. s. 299, 300, 301, 302 vd.
[229] Gökhan USTA 2019, age. s. 129, 130, 131; Türk Standardları Enstitüsü, a.g.b. 30; M. Alparslan AKYILDIZ ve Doğukan SANER 2020, age. 62; Bünyamin DEMİR 2020, age. s. 191, 192, 193 vd.

Hedef sistemde filtrelemeye yönelik bir açık varsa, hedef sisteme bir dosya yüklendiğinde ve örneğin FTP uygulamasına yüklenen bir film dosyasında da benzer sonuçlar oluşabilecektir. Bu yöntemle direkt olarak malware gönderilebileceği gibi malwarelere ek olarak ya da tekil biçimde dosyalara zararlı kodlar da gömülebilir ve sitenin diğer ziyaretçilerine karşı saldırılar gerçekleştirilebilir.[230] Spam mail/mesajlar ile gönderilen linklere tıklandığında da benzer durumlar gerçekleşebilir.[231] Bilinmesi gerekir ki hedef sunuculara bir malware ya da kod enjekte edildiğinde bunun çok ciddi sonuçları doğabilmektedir. Bu yöntemler kripto para hırsızlığından, e-ticaret müşterilerinin kart ve sair bilgilerinin çalınmasına kadar pek çok organize suçta da kullanılmaktadır.[232]

XSS ve benzeri saldırı tiplerinde hedef sistemler üzerinden üçüncü taraflara saldırıda bulunulabiliyor olmasının yanında, üçüncü tarafların sistemlerine de bu sayede erişilebilir. Hedef sisteme yapılan enjeksiyondan sonra üçüncü taraf sistemlere erişmeyi amaçlayan saldırılarda temel hedef ziyaretçi cookieleridir. Web'de WWW-http teknolojisi kullanıldığı ve http'ye dayalı iletişimde de sunucular istemciden gelen her istekte istemciyi ''*yeniden algıladığı ve önceki istemci bilgisini doğrudan tutmadığı*'' için cookie kullanım ihtiyacı doğmuştur. Cookie kullanımı ile web sitesinde gezinirken veya cookienin işlevine göre web sitesi ile iletişim koptuktan ve tarayıcı kapatıldıktan sonra dahi istemci bilgilerinin kayıtlı şekilde tutulması sağlanır. Web sitesinde gezinirken kullanılan cookieler session cookie olarak adlandırılır ve bunlar iletişim koptuktan/siteden çıkıldıktan ya da duruma göre tarayıcı kapatıldıktan sonra silinirler. Tarayıcı kapatıldıktan sonra da kayıtlı tutulan cookielere ise permenent cookie denilmektedir.[233] Örneğin bir alış veriş sitesinde seçilen ürünlere dair sepet bilgisi, tarayıcı tarafından kaydedilir ve karşı taraftaki web sunucu ile session ID üzerinden yapılan eşleşmede sunucuya bu kaydedilmiş bilgiler gönderilerek, site

[230] Hamza ELBAHADIR 2021, age. s. 173, 174; Onur AKTAŞ 2020, age. s. 343, 344 vd.
[231] Bünyamin DEMİR 2020, age. s. 259, 260 vd.
[232] INTERPOL'ün bu spesifik örneklere dair gerçekleştirdiği operasyonlara dair bkz. INTERPOL, Cybercrime Operations, https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations, (ET: 02.03.2022).
[233] Gökhan USTA 2019, age. s. 117, 118, 119, 120, 121; ''*Cookiler, ziyaret edilen web siteleri tarafından istemcinin internet tarayıcısına cookie jar şeklinde yüklenen text bazlı dosyalardır*.'' M. Alparslan AKYILDIZ ve Doğukan SANER 2020, age. s. 13; ''*Cookie'ler, web sunucuları tarafından, sunucuya bağlanma isteği gönderen istemci bilgisayarlara text dosyası olarak bırakılır. İstemci bilgisayar, web sunucusuna ikinci defa bağlanmak istediği zaman, bilgisayara bırakılan Cookie dosyası, sunucu bilgisayara gönderilir. Böylece tanımlama işlevi gerçekleştirilmiş olur.*'' Hamza ELBAHADIR 2021, s. 82.

kullanıldığı sürece ‘’*session ID’ye dair sepet bilgisini göster*‘’ denilir.[234] Sunucuya XSS ile enjekte edilen kod suretiyle session ID çalınırsa, mağdurun oturum zamanı bitmeden saldırganın bu ID’yi kendi ID’si gibi gösterecek aracı yazılımlar kullanması suretiyle sunucudaki session ID ve saldırganın taklit ID’si eşleştirilebilir, bu sayede de şifre ve sair bilgi öğrenilmeden yetkisiz olarak kullanıcı ara yüzlerine/sistemlere erişilebilir.[235]

2.3.1.6. Phishing

Phishing; hedef kişilerin kimlik, bankacılık, şifre ve sair bilgilerini ele geçirebilmek için yapılan ve içerisinde pek çok hacking yöntemini barındırabilen ve özünde de aldatıcılık içeren faaliyetler topluluğudur.[236] Phishingde en çok kullanılan yöntem, sahte internet site/uygulamaları internet ağına sokularak, internet kullanıcıların bu sahte platformlara çekilmesi ve farkında olmadan gerçek platformmuş gibi bu noktalarda işlem gerçekleştirmelerinin amaçlanmasıdır. Aşağıda mitm(*man in the middle*) yöntemi açıklanırken detaylandırıldığı üzere, üçüncü taraf bir bilişim sistemine erişilerek istemciler farklı noktalara çıkartılabilir ve bu noktalar üzerinden bilgileri çalınabilir. Örneğin istemci DNS, proxy ve sair ‘’aradaki‘’ sunucular ya da farklı sistemler vasıtasıyla sahte sitelere çıkartılabilir ve bu noktalarda yaptığı işlemler dolayısıyla verileri çalınabilir.

Hacker yukarıda bahsedilen enjeksiyon saldırılarını kullanarak bir siteyi hackledikten sonra da phishingi gerçekleştirebilir. Böylece hacklenmiş siteyi ziyaret eden internet kullanıcılarını, çeşitli noktalara tıkladıklarında veya salt siteyi ziyaret ettikleri anda kendi kontrolündeki üçüncü taraf bir siteye ulaştırabilir. Örneğin internet kullanıcısı abcdefg.org sitesine ulaştığında, bridge oluşturulmuş gibi direkt olarak aynı sekme üzerinden sahte internet sitesi olan abcdefg.pro sitesine yönlendirilir. Alan adının sonundaki en üst seviye alan adındaki(*.org*) değişikliği fark etmeyen kullanıcı, her şeyi benzer olan bu sahte siteye çekilir ve eğer bu sitede bilgilerini girerek işlemler gerçekleştirirse, hacker phishing yöntemiyle bu bilgileri ele geçirmiş olur. Kullanılan internet ortamı eğer alenen internette barındırılıyor ise herkes bu noktayı bilebileceğinden, esasında hackerların şifre girildikten sonra karşılaşılan kullanıcı ara

[234] Sunucudan veri dönüşü hiç beklenmeden verilere erişilmek istenildiğinde ise cookie kullanımının ötesinde cache/önbellek veri kayıt işlemi tarayıcılar tarafından gerçekleştirilebilir.
[235] M. Alparslan AKYILDIZ ve Doğukan SANER 2020, age. 65.
[236] Gunter OLLMANN 2007, age. s. 4.

yüzünün birebir kopyasını yapması da mümkündür. Bu şekilde örneğin sahte e-ticaret sitesinde üye girişi sonrası öğrenilebilen kişisel verilerinin ötesinde, hacker mağduru eğer gerçek siteye yönlendirmez ve phishing'e devam eder ise sahte kullanıcı ara yüzünden mağdurun alışveriş yapması ve kredi kartı bilgilerinin elde edilmesi de mümkün olacaktır. Fakat genellikle phishingde bu kadar ileri gidilmez ve giriş bilgileri elde edildikten sonra mağdurlar gerçek internet sitelerine/kullanıcı ara yüzlerine yönlendirilirler.[237]

Gerçeğine benzeyen sahte uygulamaların/sitelerin kullanımı veya gerçeği olmayan uygulamaların sahtesinin üretilerek kullanıcılara sunulması yaygın bir yöntemdir. Hackerlar bazen internet kullanıcılarının kendiliğinden bu tür tuzaklara düşmesini beklemeden, ortaya bir yem atabilir ve örneğin bir bankadan geliyormuş gibi sahte bir mail atılarak ''*şifrenizin değiştirilme süresi geldi, aşağıdaki linke tıklayınız*'' gibi beyanlarda bulunabilirler. Mağdur linke tıkladığında zararlı kod ve/veya yazılımlara maruz kalabilir ise de bu yöntemin phishing ile bağlantılı noktası, mağdurun linke tıkladıktan sonra eriştiği URL'de şifresini girmesi ve kendisine yeni bir şifre belirlediğini zannederek işlemlerini tamamlamasıdır. Bu sayede de aldatma sonucu şifreleri ele geçirilmiş olur.[238] Genellikle phishing öncesinde sosyal medya gibi açık kaynaklardan bilgi edinilmeye çalışılır, sosyal mühendisliğe başvurulur ve hatta posta kutusu ya da çöpler de karıştırılabilir ve eğer yukarıdaki örnekteki gibi mağdura banka izlenimi verilecek ise mağdurun hangi bankanın müşterisi olduğu inandırıcılık açısından öğrenilir.

Phishing başlığı altında açıklanması uygun olacak sosyal mühendislik yöntemleri, yukarıda zikredilen spam mail ya da sahte internet sitesi faaliyetlerini ve siber uzay haricindeki toplumsal düzende gerçekleştirilen aldatma, tuzağa düşürme ve bilgi edinme yöntemlerine dayanan faaliyetler bütünüdür. Sosyal mühendislikte temel unsur, kurbanın manipüle edilmesi ve saldırganın gerçek niyetini bilmediği için kurbanın manipülasyon doğrultusunda faaliyetlerde bulunmasıdır. Yani birinin iş ortağının bilerek hackerlara bilgi vermesi ve suç ortağı pozisyonuna girmesi sosyal mühendislik sayılmayacak, iş ortağının bu bilgileri hackera değil banka görevlisine verdiğini sanması ve bu yönde aldatılması durumunda ise sosyal mühendislik gündeme gelecektir. Bu açıklamalardan anlaşılacağı üzere phishing içerisinde sosyal

[237] Gunter OLLMANN 2007, age. s. 5.
[238] Cemal ARAALAN 2021, age. s. 78, 79, 80 vd.; Gunter OLLMANN 2007, age. s. 5; Şeref SAĞIROĞLU 2018, age. s. 31.

mühendislik tekniklerini de barındıran bir yöntemdir ancak phishing sosyal mühendisliğin sadece bir boyutunu oluşturmaktadır. Zira sosyal mühendislik yöntemleriyle yalnızca mağdurun bilgileri öğrenilmeye çalışılmamakta, salt malware enjeksiyonu da yapılabilmektedir. Örneğin sahte bankadan gelen bir dokümana tıklandığında dekont yerine spyware indirilebilir.[239]

2.3.1.7. Spoofing

Bilişim sistemleri genellikle küçük çaplı ağlar üzerinde bulunur ve örneğin internet üzerinden yapılan iletişimde küresel ölçekte bu ağlar arası iletişim gerçekleşir. Lakin ağlardaki her bilişim sistemi internet trafiğine açık şekilde ya da internetteki her istemciden veri alacak şekilde konumlandırılmaz. Firewall uygulamalarının temel mantığı bu sınırlandırılmış erişimin aşılmamasını sağlamak olup, bu duruma yönelik firewall dışında pek çok önlem daha alınabilir. Eğer bir hacker ağdaki bu sınırlı erişime sahip sistemlere ağ bağlantısı/internet üzerinden istek, veri paketi, kod, zararlı yazılım göndermek veya bir şekilde bu sisteme sızmak istiyorsa, önce bu sınırlı erişimi aşması gerekecektir.

Eğer sızılmak istenilen sistemin bulunduğu ağın topolojisi çıkartılırsa, ağdaki IP ve MAC'ler taklit edilerek firewall atlatılabilir ve bu şekilde ağdaki dışarıya kapalı sistemler ile veri iletişimi sağlanabilir. Böyle bir durumda erişim şifrelenmiş ise brute force saldırıları ile şifreler de kırılabilir ve hacking amacına ulaşabilir.[240] Önemli olan şudur ki şifresi bilinse bile firewall ancak belirli MAC ve IP adreslerinin o sistem ile iletişim kurabileceğini belirlemiş olabileceğinden, bu noktada yetkili gibi görünmek ve MAC-IP taklidini gerçekleştirmek çok önemlidir.[241] İşte bu taklit işlemlerine spoofing denilmektedir.

2.3.2. Araya Girme Suçu ile İlişkili Hacking Yöntemleri

İlgili bölümde detaylı olarak açıklandığı üzere araya girme suçundaki temel özellik trafiğin, veri iletişiminin gönderici-alıcı tarafı olan sistemlere girilmeden/erişilmeden teknik araçlarla izlenmesidir. Bu suç tipi salt internet ve

[239] Ayrıca bkz. Onur AKTAŞ 2020, age. s. 143, 144, 145; Gunter OLLMANN 2007, age. s. 11; Teemu VAİSANEN, Lorena TRİNBERG ve Nikolas PİSSANİDİS 2016, age. s. 27; Mustafa Yasir ŞENTÜRK 2018, age. s. 96.
[240] Gökhan USTA 2019, age. s. 101.
[241] Besim ALTINOK 2021, age. s. 97, 98, 99 vd.

benzeri yapılar yönünden geçerli değil ise de aşağıda internet ile bağlantılı network teknolojileri vasıtasıyla gerçekleştirilen hacking yöntemlerinden örnekler verilmiştir.

2.3.2.1. Man In The Middle (*MITM*)

Araya girme suçu ile ilişkili en temel yöntem, ağ iletişimindeki aracı sistemler üzerinden veri trafiğini izlemektir. Ağ yapısı, en az iki bilişim sisteminin birbiri ile kablosuz veya kablolu yöntemler vasıtasıyla bağlı olması ve iletişim kurabilir durumda bulunmasıdır. Çoğu zaman ise bu tür yerel ağ yapılarında ikiden fazla ve kurumsal ağ yapılarında ise onlarca bilişim sistemi birbirine bağlıdır. Kablolu bağlantılarda switch/hub cihazları, routerlar veya bu özellikteki modemler, bilgisayarlar, yazıcılar, sunucular ve sair pek çok sistem bağlantı halindedir. Kablosuz bağlantılarda buna tabletler, telefonlar ve IoT sistemler de eklenir. Böyle bir yapıda sistemler Ring topolojiye göre bağlı değilse ve verileri birbiri üzerinden geçirmiyorsa, genellikle tüm sistemler swithc/hub/modeme bağlı durumdadırlar ve iç iletişimde switch/modem, WAN'a çıkışlarda da router/modem ''aradaki-ortadaki'' sistem konumundadır. İnternet trafiğinde ise yerel ağdan çıkış yapıldığı andan itibaren internet omurgası üzerindeki erişim sağlayıcı routerları ve erişim sağlayıcıların diğer bağlantı sistemleri üzerinden nihai hedef sunucuya doğru akan veriler, daha pek çok üçüncü taraf ara sistem üzerinden geçirilebilir. Proxy, VPN, DNS sunucular, bridge oluşturulmuşsa bu aracı sistemler, P2P ağlardaki eş bağlantı noktaları gibi internet iletişiminde bir çok ''aradaki-ortadaki'' sistem mevcuttur.

Elektronik haberleşme altyapısına dayalı iletişimde veriler, taraflar arasındaki veri trafiğinin üzerinde bulunan bu aradaki sistemler üzerinden geçer. İşte bu yüzden bu aradaki sistemler vasıtasıyla veri trafiği, iletişimin direkt tarafı olan istemci-nihai sunucu(*gönderici-alıcı*) sistemlere erişilmeden izlenebilir. Bu ara konumdaki sistemleri yetkili olarak kontrol eden veya bir şekilde bu sistemlere sızmış ve bu sayede trafiği izleyebilecek olan kişilere ''ortadaki adam'' yani man in the middle denilir.

Bazı durumlarda hacker, aradaki sistemlerde yetkili olarak bulunmaz ve bu sistemlere yetkisiz erişim sağlayarak/sızarak, bu sayede mitm konumundan trafiği izler.[242] Örneğin hacker ilk olarak DNS sunucuyu hackler ve IP-alan adı eşleştirmesi

[242] Böyle bir durumda aradaki sistemlerin yetkililerine karşı ''yetkisiz erişim'' suçuna konu bir fiilin gerçekleştirildiği, iletişimin tarafı olan istemci-nihai sunucu sistemlere yönelik ise ''araya girme'' suçuna konu fiillerin gerçekleştirildiği unutulmamalıdır.

yaparak istemciyi ulaşmak istediği alan adına ulaştırması gereken DNS sunucunun düzgün çalışmamasını sağlar. Hacker bu ihtimalde trafiğe konu verilerin DNS sunucular üzerinden erişilebilen kısmını, direkt olarak sızdığı DNS sunucu üzerinden izleyebilir. İkinci olarak hacker gerçek DNS sunucuyu hacklemez ve mitm konumunda bulunan DNS sunucuyu taklit ederek, istemci trafiğini DNS sunucu yerine kendisine çekebilir. İşte bu noktada hacker bu sahte DNS sunucuları da mitm konumunda kullanabilir ve trafiği bu ara sistem üzerinden izleyerek, istemciyi ulaşmak istediği gerçek sunuculara tıpkı DNS sunucunun yapması gerektiği gibi ulaştırabilir. Bu sayede istemci nihai hedefine ulaştığı için saldırının farkına bile varmayacaktır. Bu tür örnekleri çoğaltmak mümkündür. Hackerın bir şekilde router'a sızması veya ağda sahte router kurarak, cihaz üzerinden geçen verileri gözlemesi ya da router üzerinden kendi kontrolündeki noktalara istemci trafiğini çıkartması da mümkündür.[243]

Mitm konumunda gerçekleştirilen dinleme/izleme faaliyetlerinde eğer orta seviye yazılımlar kullanılıyor ise bu durumlarda hacker sorunsuz olarak veri trafiğine dair genel nitelikteki bilgileri ve örneğin kaynak-hedef sistem bilgisi ile iletişim zamanını öğrenebilir. Ancak esas tehlike bu konumdaki hackerların trafiğe konu veri paketlerinin içeriğini yani paketler içerisinde gönderilen bilgileri(*örn. mesajları*) de izleyebilmesi ve anlamlandırabilmesi imkanıdır. Bunun için üst seviye paket analiz teknolojilerinin bu aradaki sistemlerde çalıştırılması gerekir.

Mitm konumunda trafikteki veri paketlerinin içeriğinin öğrenilebilmesi oldukça önemli bir hacking yöntemidir. Phishing ve benzeri bir yönteme başvurularak da istemci trafiği aldatıcı bir siteye, örneğin sahte bir Facebook giriş sayfasına yönlendirilebilir. Bu durumda da bir paket analiz yazılımına gerek kalmadan, şifreler öğrenilebilir ve istemci şifreleri öğrenildikten sonra gerçek Facebook sayfasına yönlendirilerek, saldırıyı fark etmemesi sağlanabilir.[244] Lakin bu tür yöntemlerle anlık Facebook yazışmalarının ya da VoIP konuşmalarının öğrenilebilmesi mümkün değildir. Mitm konumunda üst seviye bir paket analiz yazılımının çalıştırılması durumunda ise kriptolanmamış tüm veri bilgisinin öğrenilebilmesi, hedef sisteme herhangi bir malware enjekte etmeden mümkün olabilmektedir.

[243] Gökhan USTA 2018, age. s. 114, 115.

[244] Poongodi THANGAMUTHU, Anu RATHEE, Suresh PLANİMUTHU ve Balamurugan BALUSAMY 2020, age. s. 10; Gunter OLLMANN 2007, age. s. 23; BİLGEM, Alan Adı Rehberi, s. 29, 30, 31; Bünyamin DEMİR 2020, age. s. 158; Gökhan USTA 2018, age. s. 94, 95.

Eğer hacker trafiği aradaki sistemler üzerinden izliyor ise bu noktada saldırının başarıya ulaşamaması için iki ihtimal bulunmaktadır. Bunlardan ilki, mitm saldırılarında büyük ölçüde etkili olan ‘’veri trafiğini‘’ kriptolamaktır. VPN kullanımında ve eğer site/uygulamada SSL[245] bulunuyorsa, bu tür yapılar veri trafiğini kriptolayacağı için trafiği izleyenler verilerin kriptolanmış hallerini görür fakat bundan bir anlam çıkartamazlar. Lakin SSL kullanımında eğer hacker bu SSL'yi taklit ediyorsa, istemcinin gönderdiği trafiği kriptosuz şekilde izleyebilecektir. Yine SSL ya da VPN kullanımlarında hackerın kriptolu verileri gözlemesi ve bilahare kriptoyu çözmesi de şüphesiz ki zor da olsa mümkündür.[246] Eğer hacker trafiğe dair kriptolamayı aşabiliyor ve ayrıca güçlü bir paket analiz teknolojisi kullanarak veri paketlerinin içerisindeki bilgilere de erişebiliyor ise bu noktada doğrudan trafikteki veri dosyalarının kriptolanması ve örneğin kriptolu mail teknolojilerine başvurulması gerekir.

2.3.2.2. Sniffing

Yerel ağdaki iletişimin izlenebilmesi için daima aradaki sistemleri kontrol etme ve mitm konumunda bulunmaya gerek yoktur. Mitm konumunda bulunmadan ağdaki veri trafiğini izlemeye dair faaliyetler genel olarak sniffing şeklinde adlandırılır. Sniffingde ilk yöntem, yerel ağ içerisindeki bir sistem üzerinden sniffing saldırısı başlatılmasıdır. Sniffing'de yerel ağda yetkili olarak bulunan bir kişi sniffing saldırısı başlatabileceği gibi[247] yerel ağdaki bir sistemin WAN üzerinden hacklenerek ağda sniffing saldırısı başlatılması ve verilerin internet vasıtasıyla hackera gönderilmesi de mümkündür. WAN üzerinden ağdaki sistemlere erişilememesi için firewall, ağ içerisinde sniffing atakları yapılamaması için de sniffer yazılımlarını engelleyen ayarlar ya da DLP vb. teknolojiler mevcuttur.

Yerel ağdaki bir sistem üzerinden yapılan sniffing saldırıları, eğer ağda bunu engelleyecek bir önlem yok ise doğru paket analiz yazılımları kullanıldığında hackerın

---

[245] TCP/IP protokoller kümesinin bir bileşeni olan HTTP, web sitelerindeki iletişimde kullanılır. Bu konuda ayrıntılı bilgi için bkz. Toros Rifat ÇÖLKESEN 2018, age. s. 78, 79; Cebrail TAŞKIN 2018, age. s. 147 / HTTP'nin işletilmesiyle gerçekleşen iletişimde veri trafiği SSL ile kriptolanır ise http'ye ‘’s‘’ eki gelmekte ve HTTPS oluşmaktadır. SSL konusunda detaylı bilgi için bkz. Murat CENK (2019), ‘’Siber Güvenlikte Kriptografi‘’, İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 2,* Ed. Şeref Sağıroğlu, Mustafa Şenol, ss. 63-82, Grafiker, Ankara, s. 71-72 / Aynı durum FTP veya SMTP protokollerinin işletilmesinde de geçerli olup, SSL'nin çalıştırılması durumunda bunlara da ‘’s‘’ eki getirilir. Bkz. Mustafa Yasir ŞENTÜRK 2018, age. s. 58.

[246] Bünyamin DEMİR 2020, age. s. 158, 159 vd.

[247] Veri ihlallerinin büyük kısmının içeriden yapılan sızdırmalar sonucu oluştuğu yönünde bkz. Gökhan USTA 2018, age. s. 17.

ağdaki tüm veri trafiğini izlemesi ile sonuçlanır. Mitm saldırılarından farklı olarak yalnızca belirli sistemlerin değil tüm ağın trafiğini izleme imkanı sağlayan sniffing saldırıları, kablolu veya kablosuz ağlarda gerçekleştirilebileceği gibi yerel ağın sanallaştırılmış bölümlerinde(*VLAN*) de gerçekleştirilebilir. Eğer veri trafiği kriptosuz olarak yapılıyor ise[248] sniffing sonucunda şifreler, mesajlarda geçen önemli bilgiler ve VoIP üzerinden iletilen kritik bilgiler elde edilebilir.[249]

Eğer hacker kablolu ağ yapılarında ağa bağlı değilse, ağda sniffing saldırısı başlatabilmesi zordur. Zira hackerın kendi kablosunu switch/modem portuna bağlaması çok zor olduğundan evvela ağdaki bir sistemi hacklemesi gerekecektir. Lakin ağdaki sistemler wi-fi bağlantı noktaları(*bu genelde modemdir ve modem aynı zamanda router ve aynı zamanda dhcp sunucu işlevi görür*) ile kablosuz şekilde bağlanmışsa bu durum çok daha kolay olacaktır. Zira kablosuz ağa bağlantı şifrelenmiş olsa bile bu şifrenin brute force saldırıları ile kırılması mümkündür. İkinci olarak wi-fi teknolojilerinde ağ içerisinde dönen trafik, genellikle WEP ya da WPA algoritmalarının işletilmesi ile ağ dışına karşı kriptolanmakta ise de burada kriptolanan veriler, ağa dahil olan sistemlerden iletilen verilerdir. Bu sebeple ağa bağlanmak amacıyla bağlantı noktası/modeme gönderilen veri paketleri kriptolanmaz. Öyleyse ağa bağlanmadan, bağlantı noktası ile istemci arasındaki trafik izlenir ise bu noktada şifre de elde edilebilir ve böylece (*eğer ağa dahil olabilecek statik MAC adresleri belirlenmemişse*)[250] hacker wi-fi ağına erişerek tüm ağ trafiğini ağ içerisinden başlatacağı sniffing saldırısı ile izleyebilir.[251]

Sniffingde ikinci yöntem ağa dahil olmadan, ağ dışındaki bir sistem üzerinden trafiğin izlenmesidir. Kablosuz ağ yapılarında veriler elektromanyetik dalgalar aracılığıyla iletildiğinden,[252] veri paketlerinin ağa dahil olunmadan da yakalanması ve analizi mümkündür. Ağ trafiği eğer kriptosuz yapılıyor ise direkt olarak, kriptolu bir trafik varsa bu kripto kırılarak, ağa dahil olmadan ağ içerisindeki trafik sniffing yoluyla izlenebilir. Ağ dışından veri trafiğinin izlenememesi için

---

[248] Veri trafiğinin kriptolanmasının sniffing saldırılarının önüne geçebileceği yönünde bkz. Hamza ELBAHADIR 2021, age. s. 213.

[249] Bünyamin DEMİR 2020, age. s. 89; BİLGEM (2019), Kablosuz Ağların İşletimi Rehberi, s. 31; Wikipedia, Packet Analyzer, https://en.wikipedia.org/wiki/Packet_analyzer, (ET: 03.03.2022); Wikipedia, Sniffing Attack, https://en.wikipedia.org/wiki/Sniffing_attack, (ET: 02.03.2022); Mustafa Yasir ŞENTÜRK 2018, age. s. 25, BİLGEM (2020), VOIP Rehberi, s. 58, 59; Sniffing yöntemine ve pasif-aktif olarak hub ve switch üzerinden gerçekleştirilen tekniklere yönelik ikili anlatıma dair bkz. Sean Philip ORİYANO 2014, age. s. 279, 280, 281.

[250] MAC adresleri de değiştirilebileceğinden, aslında bu da kesin bir çözüm değildir.

[251] Gökhan USTA 2018, age. s. 127, 128, 129, 130 vd.; Besim ALTINOK 2021, age. s. 29.

[252] BİLGEM, Kablosuz Ağların İşletimi Rehberi, s. 30.

dalgaların/sinyallerin yayıldığı alana yabancı bilişim sistemi sokulmaması gerekir. Örneğin komşular ya da sokaktan geçenlerin wi-fi iletişimindeki sinyalleri yakalayamıyor olması, buna dair ev içerisinde önlem alınması ya da sinyal seviyesinin buna göre ayarlanmasına bağlıdır.[253]

Hackerın kablosuz ağlara dahil olmak yerine istemcileri yanlış biçimde kendi ağına dahil etmesi ve bu şekilde sniffing saldırısı gerçekleştirmesi de mümkündür. Mitm saldırısını da andıran bu durum, üçüncü tür sniffing yöntemi olarak adlandırılabilir. Örneğin wi-fi ağına dahil olmak isteyen sistemler, bağlantı kuracakları bağlantı noktasının/modemin MAC adresini değil, SSID'yi görürler ve buna bağlantı isteği yollarlar. Eğer hacker aynı şekilde isimlendirdiği sahte bir bağlantı noktasını paylaşıma açarsa, kişiler yanlışlıkla sahte ağa dahil olabilecektir. Bu durum iki şekilde gerçekleşebilir. Evvela kamuya açık şifresiz toplu taşıma ya da restoran/AVM ağları bu saldırıya konu olabilir. Hacker bu bağlantı noktasını taklit ederek kişileri sahte ağına bağlayabilir ve bu şekilde trafiği izleyebilir. İkinci olarak, hacker şifreli bir ağı da taklit edebilir. Şifresini bildiği için sahte bağlantı noktasının şifresini de aynı yapabilir ve istemcilerin şüphelenmemesini sağlayabilir. Yine DoS/DDoS saldırıları ile gerçek bağlantı noktasına dair SSID devre dışı bırakılabilir ve yalnızca sahte bağlantı noktası bağlanılabilir konumda olduğundan, istemciler bu saldırgan ağa bağlanabilir. Bu şekilde de şüphesiz ki sahte ağa çekilen kişilerin ağ dışına gönderdikleri veri paketleri ve örneğin internet kullanımlarına dair trafik izlenebilecektir.[254]

2.3.2.3. MAC-ARP Spoofing ve MAC Flooding

Yerel ağda Ethernet üzerinden yapılan ağ iletişimi, sistemlerin sahip olduğu Ethernet kartlarına işli MAC adresleri vasıtasıyla gerçekleşir ve veriler temelde ortak bağlantı noktası(*switch/hub*) vasıtasıyla alıcı/hedef MAC adreslerine göre yönlendirilirler. Ağdaki sistemlerin her birinin ayrı bir MAC adresi mevcut olup bu iletişimin doğru işlemesini sağlayan, MAC tablosu tutan ve gönderici-alıcı tarafları eşleştiren Ethernet protokollerinin işletilmesidir. Bu protokoller bir şekilde şaşırtıldığında ya da bozulduğunda ise veriler salt gitmesi gereken noktalara değil,

[253] Gökhan USTA 2018, age. s. 135.
[254] Sahte wi-fi bağlantı noktalarına dair ayrıntılı bilgi için bkz. Besim ALTINOK 2021, age. s. 91, 92 vd.; BİLGEM, Kablosuz Ağların İşletimi Rehberi, s. 31, 32.

hackera da gidebilir. Verilerin yerel ağda yaratılan hata sebebiyle hackera da iletilmesine dair bu başlık altında iki temel yöntemden bahsedilecektir.

İlk olarak yerel ağda yetkili olarak bulunan ya da bu ağdaki sistemlerden birini hackleyerek kontrolü altına alan hacker, kontrolü altındaki sistemin ayarlarını değiştirerek ağdaki bazı verilerin istenmeden kendisine gönderilmesine neden olabilir. Bu durumda hacker kontrolü altına aldığı bir bilgisayarın MAC adresini ve/veya port numaralarını değiştirerek, ağda bu noktalara gönderilen verilerin kendisine iletilmesini sağlayabilir. Zira MAC tablosu eğer iki farklı bağlantı noktası aynı MAC adresine sahip olmuş ise karışıklık çıkmaması için önceki bağlantı noktasını silmektedir. Bu sayede düzgün işlemeye çalışan Ethernet protokolü, istemeden tam tersi bir duruma sebep olur. Bu saldırı tipine MAC spoofing denilmektedir.[255] Böylece ağdaki X ve Y noktaları arasında iletilmesi gereken trafik, hackerın önceden ele geçirdiği aynı ağdaki Z noktasına iletilir ve hacker ne X ne de Y sistemlerine erişmeden, aradaki trafiği izlemiş/öğrenmiş olur. Bu durumda veriler doğrudan hackera iletildiği için genellikle bir paket analiz yazılımı kullanılması da gerekmez.

Eğer bir yerel ağ internete/WAN'a router vasıtasıyla geçiş sağlıyor ise WAN üzerindeki bağlantıda router/modemlerin IP adresleri, yerel ağda ise DHCP sunucunun ya da bu işlevi gerçekleştiren modemin dağıttığı NAT/iç IP adresleri bulunacaktır. DHCP sunucular veya bu işlevi gerçekleştiren sistemler, ağdaki her bir sisteme IP dağıtımı yaparken bunu her sistemin kimlik bilgisi olan özgün MAC adreslerine göre yapar. Modem/router WAN üzerinden gelen verileri alıcılarına ulaştırırken, içeride bu iç IP adreslerini kullanarak hedefini bulur. Yerel ağdaki sistemler arasındaki iletişim ise yukarıda belirtildiği gibi MAC adresleri üzerinden gerçekleşir. İç IP'lere karşılık gelen MAC adreslerinin ağ içi iletişimde bilinir olması için ise genellikle ARP protokolü kullanılır. Eğer saldırgan ağdaki kendi sisteminin iç IP'sini trafiğini izlemek istediği sistemin iç IP'si ile değiştirir ve ARP sisteminin işleyişini bu şekilde bozarsa, izlenmek istenen sisteme giden veri paketleri saldırgana gideceği için saldırgan iletişimin doğrudan alıcı tarafı olur. Buna da ARP spoofing saldırısı denilmektedir.[256]

İkinci yöntem, önemli bir hacking yöntemi olan MAC flooding saldırılarıdır. MAC tablosu sınırsız bir belleğe ve sayısız ayrı sistemin kaydedilmesine elverişli

[255] Gökhan USTA 2018, age. s. 75.
[256] Gökhan USTA 2018, age. s. 34, 35, 36, 81, 82 / ARP için ayrıca bkz. İTÜBİDB, Seyir Defteri, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/arp-(adres-%C3%A7%C3%B6z%C3%BCmleme-protokol%C3%BC), (ET: 02.03.2022).

değildir. Hacker bu işleve sahip bir yazılım kullanarak kendi sistemine çok sayıda farklı MAC adresi verebilir ve MAC tablosunun belleğinin dolup taşmasına sebep olarak, veri iletimini sağlayan Ethernet protokollerini(*ARP*) bozabilir. Bir yandan DoS etkisi yaratan bu durum, esas olarak veri iletimini yapan sisteme erişilmeden, gönderdiği verilerin izlenmesi için kullanılır. Örneğin X sistemi Y sistemine veri iletirken, Ethernet protokollerini işleten ve tabloyu tutan ortak bağlantı noktası(*örn. switch görevi gören portlara sahip modem*) bu veri trafiğinin sağlıklı işlemesini sağlar. Eğer hacker MAC flooding saldırısı yaparak bu işleyişi bozarsa, iletişimin alıcı tarafı yalnızca Y değil, hacker dahil ağdaki tüm bağlı sistemler olacaktır. MAC flooding saldırılarında spoofingden farklı olarak, verilerin elde edilebilmesi/yakalayabilmesi için genellikle saldırganın paket analiz yazılımı kullanması gerekir.[257]

[257] Wikipedia, MAC Flooding, https://en.wikipedia.org/wiki/MAC_flooding/, (ET: 02.03.2022), Gökhan USTA 2018, age. s. 34, 35, 75; Sean Philip ORİYANO 2014, age. s. 283.

BÖLÜM III

YETKİSİZ ERİŞİM SUÇUNUN UNSURLARI

3.1. NORMUN KORUMAYI AMAÇLADIĞI HUKUKSAL DEĞERLER

Bir normun(*örn. TCK md. 243*) korumayı amaçladığı değerleri ihlal etmeyen bir fiil ilgili norm nazarında hukuka aykırı olamayacağından,[258] normun korumayı amaçladığı değerlere dair açıklamaların esasında suçun hukuka aykırılık unsuru ile doğrudan bağlantısı mevcuttur.[259] Lakin ceza normları ile korunması amaçlanan hukuksal değerler suçun objektif tipikliği ve muhakemenin mağdur süjesinin tespiti noktasında da önem arz ettiğinden, işbu tezde korunan hukuksal değerler ayrı bir başlık altında incelenmiştir. Bu doğrultuda aşağıda evvela konuya dair doktrin görüşleri açıklanmış ve bilahare şahsi kanaatler aktarılmıştır.

3.1.1. Doktrin Görüşleri

Doktrinde yetkisiz erişim suçu ile korunması amaçlanan değerlere dair çok farklı görüşler mevcuttur. Aşağıda bu görüşler sıralanmıştır:

[258] Sulhi DÖNMEZER ve Sahir ERMAN (2019), *Nazari ve Tatbiki Ceza Hukuku Cilt 2*, Ondördüncü Basım, DER, İstanbul, s. 248; Zeki HAFIZOĞULLARI ve Muharrem ÖZEN (2021), *Türk Ceza Hukuku Genel Hükümler*, Onüçüncü Basım, USA, Ankara, s. 194, 195, 197 vd.

[259] Bir suçun objektif tipikliği içerisinde kalan her fiil görünüşte hukuka aykırı olmakla birlikte, yazılı bir hukuka uygunluk sebebinin bulunması ya da yazısız hukuka uygunluk sebeplerini de içerisinde barındıran bir kavram olan ‘’normun korumayı amaçladığı değerlere aykırılık teşkil etmemesi‘’ sebebiyle özünde hukuka uygun olabilir. Ancak bir fiilin hukuka uygunluğu külliyen bütün normlar nazarından değerlendirilmesi gereken bir meseledir. Tek bir ceza normu ve örneğin TCK md. 243 nazarında yapılan bir değerlendirme ise bir fiilin külliyen hukuka uygunluğunu değil, yalnızca TCK md. 243 nazarında ‘’hukuka aykırı olmadığını‘’ tespit edebilir.

1) Birinci görüşe göre suç normu ile korunan değerler başat olarak bilişim sistemlerinin güvenliği, dolaylı olarak da ilgililerin özel hayatı, kişisel verileri ve sair haklarıdır.[260] Bazı görüşler bunların arasına kamu düzeninin korunmasını da eklemektedir.[261] Yine bunlar arasında haberleşme hürriyetini/haberleşmenin gizliliğini sayan görüşler de mevcuttur.[262] Bir kısım görüşler ise bunların yanına mülkiyet ve kişilik hakkı harici sair hakları da eklemektedir.[263]

2) İkinci bir görüşe göre ise suçla korunan hukuki değer salt sistem güvenliği/dokunulmazlığı olup, özel hayatın ya da kişisel verilerin gizliliği normun koruma amacı dışındadır.[264] Korunan hukuki değerin yalnızca siber uzayın güvenli biçimde işleyişi olduğunu yönündeki görüş de bu noktada benzer bir yorumdur.[265]

3) Üçüncü bir görüş ise bilişim sisteminin somut olarak güvenliğinin değil, güvenilirliği yani insanların bu sistemlerin güvenli çalıştıklarına dair güveninin başat olarak korunduğunu belirtmektedir. Güvenilirliğe ek olarak veriler ve özel hayatın gizliliği de normun korumayı amaçladığı değerler arasında sayılmaktadır.[266] Bunlara ek olarak sair meşru değerleri zikreden görüşler de mevcuttur.[267] Aynı yöndeki bir kısım görüş, suçun topluma karşı suçlar bölümünde düzenlenmiş olmasını da vurgulayarak, bu değerlerin yanında toplumsal faydanın-toplum/kamu düzeninin de korunmasının amaçlandığını belirtmektedir.[268]

---

[260] İsmail ERGÜN (2008), *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Adalet, age. s. 88; Ali PARLAR ve Muzaffer HATİPOĞLU 2010, age. s. 3742; Ahmet GÜL (2021), *Doğrudan Dolaylı Bilişim Suçları*, Seçkin, Ankara s. 92; Ali PARLAR ve Mustafa ÖZTÜRK (2020), *Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar*, Aristo, İstanbul, s. 25, 26 / Benzer görüşler için bkz. Tunç DEMİRCAN (2007), *Bilişim Alanında Suçlar*, Selçuk Üniversitesi Soyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Konya, s. 84.

[261] Cengiz APAYDIN 2017, age. s. 51.

[262] Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1148, 1149; Hasan Burak ÖNDİN 2017, age. s. 32; Burak ÇEKİÇ 2006, age. s. 88.

[263] Fazıl GÜRLER 2013, age. s. 91; Murat Volkan DÜLGER 2022, age. s. 254.

[264] Berrin AKBULUT 2017, age. s. 118; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 895 / Yargıtay'ın da bu görüşte olduğu söylenebilir. Bkz. ''*... TCK'nın 244. maddesi ile bilişim alanında suçlar bölümünde yer alan 243. maddede olduğu gibi bilişim sistemi ve sistemin işleyişine yönelik saldırıların önlenmesi amaçlanmış olup*'' Yargıtay CGK 2019/239 E. 2021/325 K.

[265] Zeki HAFIZOĞULLARI ve Muharrem ÖZEN (2012), *Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar,* USA, Ankara, s. 441.

[266] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 233, 234; Ahmet Caner YENİDÜNYA 2005, age. s. 3; İbrahim ŞAHBAZ 2020, a.g.e, s. 3127 / Aynı yönde bkz. Doğan SOYASLAN (2020b), *Ceza Hukuku Özel Hükümler*, Onüçüncü Basım, Yetkin, Ankara, s. 661, 662 / Bu görüşe göre bilişim alanında suçların topluma değil, kişilere karşı suçlar arasında düzenlenmesi daha doğru olacaktır. Zira sahte banka kartlarına dair suçlar haricinde esas mağdur kişidir. Bkz. Doğan SOYASLAN 2020b, age. s. 658.

[267] Şaban Cankat TAŞKIN (2008), *Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları,* Marmara Üniversitesi Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul, s. 27.

[268] Ramazan DOĞAN (2014), *Bilişim Suçları,* Adalet, Ankara s. 43.

4) Dördüncü bir görüşe göre ise suç normu ile yalnızca bilişim sistemlerinin güvenilirliği korunmaktadır.[269]

5) Beşinci bir görüş ise hem sistemin güvenliğinin hem de sistemin güvenilirliğinin korunduğu yönündedir.[270] Sair bir görüş ise bunların yanında sistemdeki verilere dair hakların, haberleşme hürriyetinin ve özel hayat ile kişisel verilerin gizliliğinin de korunduğunu belirtmektedir.[271] Bunlara ek olarak sistem üzerindeki sair meşru değerleri zikreden görüşler de mevcuttur.[272]

6) Altıncı bir görüş ise normun başat olarak özel hayatın gizliliğini koruduğunu[273] ve bunun sonucu olarak siber uzayın da korunmasının amaçlandığı yönündedir.[274] Aynı şekilde başat olarak özel hayatın ve kişisel verilerin gizliliğinin korunduğunun, bilişim sistemlerinin güvenliğinin ise ikinci planda korunduğunun belirtildiği görüşler de mevcuttur.[275]

7) Yedinci görüş ise bu suç normu ile sadece mülkiyet hakkı ve sistem güvenliğinin korunduğunu belirtmektedir.[276]

8) Sekizinci görüş ise bilişim sistemleri üzerinde tasarruf edebilme yetkisinin başat olarak, dolaylı olarak ise sitemdeki verilerin korunduğu yönündedir.[277]

---

[269] Dilek GÜLER (2018), ‘’Bilişim Sistemine Girme Suçu‘’, *KTO Karatay Hukuk Fakültesi Dergisi*, C. 3, S. 2, ss. 11-38, s. 17; Muhammet Sefa ÇETİN (2021), ‘’Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu‘’, *TAAD*, C. 12, S. 45, ss. 1-28, s. 4.

[270] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 956, 957; Büşra ÖZÇELİK 2019, age. s. 43; Mehmet Bedii KAYA (2019), ‘’Hukuki Açıdan Bilişim Suçları-Siber Güvenlik ve Adli Bilişim‘’, İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 2*, ss. 213-279, Grafiker, Ankara, s. 218.

[271] Hayati PALLI (2008), *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları,* Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Erciyes, s. 150; Meral EKİCİ ŞAHİN ve Irmak KORUCULU (2019), ‘’Bilişim Sistemine Girme Suçu-Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme‘’, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan*, C. 21, Özel Sayı, ss. 585-626, s. 591.

[272] Nagihan GÜN 2020, age. s. 187, 188; Yavuz ERDOĞAN (2010), ‘’Bilişim Sistemine Girme ve Kalma Suçu‘’, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* C. 12, Özel Sayı, ss. 1363-1433, s. 1370, 1371.

[273] Hakan KARAKEHYA (2009), ‘’Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu‘’, *TBB Dergisi*, S. 81, ss. 1-24, s. 12 / Sair hakları da saymakla birlikte esas korunan değerin sanal dünyadaki özel hayatın gizliliği olduğu yönündeki görüş için bkz. Uğur İHTİYAROĞLU (2020), ‘’Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi‘’, *Hacettepe Hukuk Fakültesi Dergisi*, C. 10, S. 2, ss. 406-440, s. 409, 410, 411, 412.

[274] Ali İhsan ERDAĞ 2010, age. s. 279.

[275] Esra YAYCI (2007), *Bilişim Suçları*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara, s. 71, 72.

[276] İlker TEPE 2009, age. s. 270.

[277] Muammer KETİZMEN 2006, age. s. 98, 106.

3.1.2. Değerlendirme

Suçun korumayı amaçladığı bir değerin, suçun her işleniş biçiminde mutlaka ihlal edilebilen bir değer olması gerekir. Örneğin yaralama suçunda kişinin üzerindeki giysinin de zarar görebileceği ihtimaline dayanılarak, mal varlığının da koruma altına alındığı gibi bir yorum yapılamaz.[278] Bilişim sistemlerine yetkisiz erişim durumunda ise her daim ihlal edilebilen tek değer, sistem üzerindeki yetkiye dayalı hakkın korunması ve bilişim sisteminin yetkisiz erişimlere karşı dokunulmazlığıdır. Öyleyse yetkisiz erişim suçu ile korunan hukuki değer yalnızca (*yetkisiz olarak erişilemeyen sistemlere dair*) sistem üzerindeki yetkiden kaynaklı hak ve bundan doğan ‘’bilişim sisteminin yetkisiz erişimlere karşı dokunulmazlığı‘’ olmalıdır.[279] Suçun topluma karşı suçlar bölümünde düzenlenmiş olması yalnızca kanunun sistematiğine bağlı şekilsel bir sonuçtur. Suç bu bölümde düzenlendiği için bu suç ile spesifik olarak kamu düzeninin ya da toplumun genelinin menfaatinin daima korunduğu anlamı çıkartılamaz. Zira bilişim sistemlerine yetkisiz olarak erişilmesi durumu, bu durum bir kamu tüzel kişiliğinin yetkisindeki sistemler üzerinde gerçekleşse dahi toplumun diğer bireylerini ya da kamu düzenini ekseriyetle ilgilendirmemektedir. İstisnai olarak E-Devlet veri tabanı gibi bazı sistemlere yetkisiz erişim durumunda pekala toplum düzeni tehlikeye düşebilecek ise de bu tür durumlar her daim yaşanmamaktadır. Kaldı ki haksız fiillerden her biri geniş çerçevede devlet ve egemenliğin sahibi toplumun[280] meşru kabul ettiği değerleri ihlal ettiğinden, bu durum TCK md. 243’e has bir unsur da teşkil etmemektedir.

Bilişim sistemi veri ve donanımların ayrılmaz bir parçası olduğundan, sistemin veri boyutunun dokunulmazlığı da ‘’sistemin dokunulmazlığı içerisinde‘’ zaten koruma altındadır. Ancak verilerin ‘’bilgi‘’ boyutuyla öğrenilmesi ve buna dayalı olarak kişisel veriler, fikri-sınai haklara konu edilebilen kaynak kodlar yahut NFT

---

[278] Doktrinde her suç normunun korumayı amaçladığı bir ‘’özel‘’ hukuksal değer olduğu ve örneğin insan öldürme suçunda yaşam hakkı dışında bir değerin korunmadığı belirtilir. Bu konuda bkz. Yener ÜNVER (2003), *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, Seçkin, Ankara, s. 802 / Kanaatimizce bir suç normu oluşturulması ile korunması amaçlanan değer yani normun raito’su ile normun varlığı sonucu ihtimal dahilinde korunabilen sair değerler, suçun unsurları bağlamında aynı kefeye konulamaz. Zira örneğin yetkisiz erişim suçunda, kişisel verilere haksız erişim(*bu değere tecavüz*) hususu suçun objektif tipikliğine dahil olmadığından, suçun oluşumu bu neticeden bağımsızdır. Öyleyse kanun koyucunun suçun objektif tipikliğine dahil olmayan bir değer ihlalini korumayı amaçladığını söylemek mümkün olmamalıdır.

[279] Benzer yönde bkz. Berrin AKBULUT 2017, age. s. 118.

[280] Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2021, age. s. 6, 7, 8, 10, 154; Doğan SOYASLAN (2020a), *Ceza Hukuku Genel Hükümler*, Dokuzuncu Basım, Yetkin Ankara, s. 33, 40 vd.; Nevzat TOROSLU ve Haluk TOROSLU (2021), *Ceza Hukuku Genel Kısım,* Savaş, Ankara, s. 20, 21, 22 vd.

eserler, özel hayatın gizliliği kapsamında kalan videolar ve sair hususlar ile bunlara bağlı haklar bu suç normunun koruma alanı kapsamında değildir. Aynı şekilde sistemlerin somut bütünlüğü üzerindeki mülkiyet, zilyetlik ve sair haklar da korunan değerler arasında yer almaz. Zira en basit olarak, bir ağ bağlantısına yetkisiz olarak erişildiğinde bu sayılanlardan hiçbiri bilfiil ihlal edilmemektedir. Yine aleni alanları çeken MOBESE kayıtlarının tutulduğu veri tabanları gibi pek çok sistemde herhangi bir kişisel veri yer almayabilir.

Bilişim sistemlerinin güvenli işlediğine dair inancın yani sistemlerin güvenilirliğinin korunduğuna yönelik görüşlere de katılmıyoruz. Zira pek çok kişi sistemlerinin güvenli biçimde işlediğine inanmamakta, bu sebeple sistemlerinde çok sayıda siber güvenlik uygulaması yapılandırmakta ve buna rağmen yetkisiz erişimler gerçekleşebilmektedir. Bize göre bilişim sisteminin ancak işlemci ve ekran kartı gücüne göre belirli programları çalıştırabileceğine veya internete bağlı bir sistemin Youtube'a erişeceğine güvenilebilir. Sistemlere yetkisiz erişim yapılmayacağına dair güven ise son derece sübjektif bir nitelemedir. Bu sebeple bir ceza normunun böylesine sübjektif bir hissiyatı korumak için oluşturulması söz konusu olamaz. Hiçbir suçta böyle bir hissiyat ve örneğin insan öldürme suçunda ''insanların cinayete kurban gitmeyeceklerine dair inanç/güven'' korunmuyorken, bilişim sistemine yetkisiz erişim suçunda da ''sistemlerin dokunulmazlığına dair inancın/güvenin'' bir maddi ceza normunun koruma alanında kalmaması gerekir.

3.2. SUÇUN TİPİKLİK UNSURU

3.2.1. Objektif Tipiklik

3.2.1.1.Fail

TCK md. 243'te düzenlenen yetkisiz erişim suçunun işlenmesinde herhangi bir özel faillik durumu yoktur. Bu durum hafifletici sebep düzenlemesi, Terörle Mücadele Kanunu'ndaki ağırlaştırıcı sebep düzenlemesi ve suçun neticesi sebebiyle ağırlaşmış hali yönünden de geçerlidir. Öyleyse herkes bu suçun faili olabilir. Doktrinde de bu konuda görüş birliği bulunmaktadır.[281]

[281] Bu yöndeki görüşler için bkz. Murat Volkan DÜLGER 2022, age. s. 257; Ali Haydar DOĞU (2017), *Bilişim Hukuku*, Ekin, Bursa, s. 134; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 234; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1149; Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2012, age. s. 441; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 896; Berrin AKBULUT 2017, age, s. 120; Ali İhsan ERDAĞ 2010, age. s. 283.

TCK'nın lafzı ve ruhundan çıkan sonuç, Türk ceza hukukunda sübjektif sorumluluk esasının benimsenmiş olduğudur. Bu sebeple kast ve taksir derecesinde bir bilinç sahibi olamayacak cansız yapıların, örneğin yapay zekanın ya da hukuki bir statü olarak tüzel kişilerin bir suçun faili olması mümkün değildir. TCK md. 246 gereğince tüzel kişiler yönünden ancak güvenlik tedbirleri gündeme gelebilir.[282]

Doktrinde bu suçu işleyen faillerin ileri düzey bilgisayar/ağ bilişim bilgisine sahip oldukları yönünde[283] görüşler mevcut olduğu gibi bilişim suçlarını genel olarak gençlerin işlediği yönünde görüşler de mevcuttur.[284] Bazı görüşler ise dar anlamdaki bilişim suçlarının faillerini, hedef ve bilinç faktörleri dahilinde dörde ayırarak incelemektedir. Bu dörtlü ayrıma göre ise kimi failler bilinçsiz ve bilgisizdirler.[285] Somut gerçekler ise her türlü failin bu suçları işleyebildiğini göstermektedir.

İşbu tez kapsamında da zikredilmiş olan INTERPOL, FBI ve EUROPOL'ün operasyonlarından da anlaşılabileceği üzere, iyi derecede bilgi sahibi hackerlar da tespit edilerek yakalanabilmektedir. Ancak Türkiye özelinde içtihatlar ve basına yansıyan olaylar değerlendirildiğinde, yargılamalara konu olmuş bilişim suçlarının çok azının profesyonel hackerlar tarafından gerçekleştirildiği görülmektedir. Çoğu fail yaptığı saldırıları şahsi bilgisayarından yapabildiği ve basit bir wipe(*kalıcı silme*) işlemini akıl edemediği gibi IP adresini dahi gizlemeyi düşünemeyen faillerin yargılandığı davalara dair içtihatların sayısı oldukça fazladır. Öyleyse ya bilişim ve network teknolojilerinden gerçekten anlayan kişiler Türkiye'de bu suçları nadiren işlemektedir ya da daha kuvvetli olan olasılığa göre bu kişiler izlerini gizledikleri/sildikleri için tespit olunamayabilmektedir.

Doktrindeki görüşlerden bir diğeri; faillerin, mağdurların çeşitli sebeplerden dolayı olayları yargıya sirayet ettirmeyecekleri ve/veya ettirseler bile adli bilişimin

---

[282] Doğan SOYASLAN 2020b, age. s. 661, 662; Murat Volkan DÜLGER 2022, age. s. 259 / Yazılım şeklinde kullanılan veya yazılım, donanım ve sensörlerden oluşan robotların yahut araçların içerisinde çalıştırılan yapay zekanın bir hukuki kişiliği bulunmamaktadır. Eğer yapay zeka teknolojilerini tüzel kişiler işletiyorsa, bu durumda yardımcı çalışan ya da operatör konumundaki gerçek kişilerin sübjektif sorumluluk nazarında bir sorumluluğu doğmuyor ise yapay zekadan kaynaklı cezai sorumluluk kimseye yüklenememektedir. Bu halde de tüzel kişi aleyhine güvenlik tedbirlerinin uygulanması için TCK md. 60'ta aranan şartlar oluşmayacağından, ceza hukuku tamamen denklemden çıkacaktır.

[283] Murat Volkan DÜLGER 2022, age. s. 126, 127, 128 vd.

[284] Bahattin ALACA (2008), *Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi(Antropolojik ve Hukuki Boyutları İle),* Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji(Sosyal Antropoloji) Anabilim Dalı Yüksek Lisans Tezi, Ankara, s. 41.

[285] Fehmi Ünsal ÖZMESTİK (2015), *Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı Yüksek Lisans Tezi, İstanbul, s. 10, 11, 12 vd.

başarıya ulaşamayacağı inancıyla hareket ettikleridir.[286] Doktrinde dile getirilen sair bir görüş ise bilişim suçlarının faillerinin genellikle gerçek dünyada suç işlemekten çekinen fakat sanal dünyada rahatlıkla suç işleyebilen kişiler olduğudur.[287] Türkiye'de yapılan ve bir çok farklı üniversiteden 312 öğrencinin katıldığı bir anket çalışmasında, bu görüşlere paralel sonuçlara ulaşılmıştır. Ankete göre katılımcıların %24.68'i bilişim suçlarının tespiti zor olduğu için gerekli bilgiye sahip olsalar idi kendilerinin de hacker olacaklarını ve suç işleyeceklerini beyan etmiştir.[288] Yine başka bir ankette ''*hackerlık yapar mısınız ?*'' sorusuna evet cevabını veren azımsanmayacak bir çoğunluk mevcuttur. Bu ikinci ankette, geniş anlamda bilişim suçlarına dair de çarpıcı sonuçlar mevcut olup, katılımcılardan % 72,5'i bilgisayarında lisanssız program olduğunu belirtmiş ve bunlardan yalnızca %35.3'ünün bundan vicdanen rahatsızlık çektiği ortaya çıkmıştır.[289]

Doktrinde dar anlamda bilişim suçlarının faillerini suç işlemeye iten sebepler hakkında da çeşitli yorumlar mevcuttur. Bu suçların kazanç, şan-şöhret, intikam, vatanseverlik dürtüsü, meydan okuma, para dışında kişisel çıkar sağlama gerekçeleriyle işlendiği belirtilmektedir.[290] Bunlara istihbarat, hacktivist gerekçeler, rakipler hakkında bilgi edinme veya salt merak duygusu gibi sair gerekçeler de eklenebilir. Kanaatimizce dar anlamdaki bilişim suçlarını işleyenlerin; bilgisizce, bilgili şekilde ve ustaca hacking faaliyetlerini yürüten failler ile başkasının telefonunu alıp kurcalayan kişiler gibi herhangi bir hacking faaliyeti gerçekleştirmeyenler şeklinde ikili bir ayrıma tabi tutulması mümkündür. Hackinge başvuran fail intikamcı bir eski sevgili, kazanç arayışındaki suç çetesi üyesi, hacktivist bir bilişim dehası, terörist faaliyetlerde bulunan bir siber terörist ya da görevlerini kötüye kullanarak delil elde etmek için hukuka aykırı davranan kolluk görevlisi de olabilir. Hackinge başvurmayan bir failin de kıskanç bir eş, velayet hakkını kötüye kullanan bir baba

[286] Murat Volkan DÜLGER 2022, age. s. 126, 127, 128, 129 vd.; Ali KARAGÜLMEZ 2014, age. s. 63, 73, 74; Bahattin ALACA 2008, age. s. 52 / KVKK normları gereğince veri ihlallerinin bildirilme zorunluluğu dolayısıyla, şirketlerin saldırıları bildirmeme ihtimallerinin oranının düştüğünü söylemek gerekir.

[287] Hamit HANCI, Hilal TOKGÖZ ve İshak YAPAR (2018), ''Tıbbi Sistemleri ve Cihazları Hedef Alan Siber Saldırılar'', *Adli Bilimler Dergisi* C. 17, S. 1 ss. 32-39, s. 43.

[288] Burak Tunç BİLEK (2012), *Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri*, Gazi Üniversitesi Bilişim Enstitüsü Bilgisayar Eğitimi Anabilim Yüksek Lisans Tezi, Ankara, s. 75.

[289] Hamit HANCI, Hilal TOKGÖZ ve İshak YAPAR 2018, age. s. 48.

[290] Ali KARAGÜLMEZ 2014, age. s. 63; Hikmet DİJLE ve Nurettin DOĞAN (2011), ''Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı'', *Bilişim Teknolojileri Dergisi*, C. 4, S. 2, ss. 43-54, s. 43; Hasan Burak ÖNDİN 2017, age. s. 14.

yahut hakkı olmadığı halde öğrencilerinin telefonlarını karıştıran bir öğretmen olması mümkündür.

Bu noktada es geçilmemesi gereken ve bilişim suçlarının failleri bakımından onları suç işlemeye iten bir diğer sebep ise kanaatimizce sanal alemde işlenen pek çok suçun, toplum nazarında kayda değer bir haksızlık olarak görülmemesidir. Örneğin bir üniversite bünyesinde gerçekleştirilen ankette, bilişim sistemine yetkisiz olarak erişmek ve bir zarar vermeden sistemden çıkmak en hafif suçlar arasında görülmüştür.[291]

3.2.1.2. Mağdur

Bir suçun mağduru, suç normu ile korunan ve suçun işlenmesi ile zarar gören hukuksal değerlerin sahibidir.[292] Suçtan zarar gören ise suçun işlenmesi sonucu herhangi bir meşru menfaati zarar gören kişidir. Yetkisiz erişim suçunda, suçun mağduru herkes olabilir.[293] Doktrindeki baskın görüş bu olmakla birlikte ayrık görüşlerden ilki, mağdurun kamu idaresi olduğu ve fertlerin ise ancak suçtan zarar gören konumunda bulunabileceğidir.[294] İkinci ayrık görüş ise mağdurun, oluşan neticeye göre toplum da olabileceğini belirtmektedir.[295]

Mağdur sıfatı daima değilse de gerçekten de milli güvenlik yahut kamu düzenini bozan saldırılar yönünden, toplumsal yapının hukuki teşkilatlanmasını oluşturan devlet tüzel kişiliği üzerinde oluşabilir. Örneğin E-Devlet veri tabanına hackerlar tarafından sızılması ve pek çok bilginin ele geçirilmesi durumu bu tür bir mağdur sıfatını doğurabilir. Böyle bir durumda verileri çalınan fertler ise suçtan zarar gören olacaktır. Yine E-Devlet sunucuları üzerinde hak sahibi olan ve/veya sunucuları işleten tüzel kişilerin de böyle bir durumda mağdur yahut suçtan zarar gören sıfatı oluşacaktır. Tüzel kişilerin yetkisiz erişim suçunun mağduru olup olamayacağı konusu aşağıda detaylı olarak değerlendirildiğinden, bu noktada daha fazla açıklamada bulunulmamıştır.

---

[291] Çığır İLBAŞ 2009, age. s. 47.
[292] Aynı yönde bkz. Tuğrul KATOĞLU (2012), ‘’Ceza Hukukunda Suçun Mağduru Kavramının Sınırları‘’, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C. 61, S. 2, ss. 657-694, s. 660, 661.
[293] Hasan GERÇEKER (2020), *Yorumlu-Uygulamalı Türk Ceza Kanunu*, Seçkin, Ankara, s. 2152; Murat Volkan DÜLGER 2022, age. s. 266; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 234, 235; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 897.
[294] Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2012, age. s. 441.
[295] Berrin AKBULUT 2017, age. s. 121.

Bu suçta mağdurun herkes olabileceği noktasındaki baskın görüşün aksine, mağdur nitelemesinin nasıl yapılması gerektiği konusunda doktrinde çok farklı görüşler mevcuttur. Bir görüşe göre bilişim sisteminin güvenliğinin ihlali sonucunda meşru yararları zarara uğrayan kişiler mağdur sıfatına sahip olacaktır.[296] Aynı yöndeki diğer görüşler de mülkiyet gibi belirli hakların sahipliği ile sınırlandırmadan, meşru yararları/hakları ihlal edilenlerin mağdur olacakları yönündedir.[297] Sair bir görüş ise bu meşru yararları ‘’yetkisiz kişilerin erişimine kapanmış‘’ bir bilişim sistemi üzerindeki mülkiyet, zilyetlik ve kiracılık hakkına indirgemiştir.[298] Başka bir görüşe göre ise sistemler üzerinde çeşitli hakların sahiplerinin yanında, sistemlerde işlenen verilerin sahipleri de bu suçun mağduru olabilirler.[299]

3.2.1.2.1. Değerlendirme

Bir bilişim sistemine yetkisiz olarak erişmek demek, ‘’*donanım + veri yani somut ve soyutun birleşimi*‘’ şeklinde anlaşılması gereken bir yapıya yetkisiz biçimde dahil olmak ve aktif ya da pasif çeşitli eylemlerde bulunmak demektir. Detayları aşağıda hareket ve neticenin açıklandığı alt başlıklar altında aktarılmış olan bu eylemler, ağ yapılarında ya da ağ bağlantısı olmadan tek başına çalışan sistemlerde veya birden fazla veri depolama-işleme birimine sahip sistemlerin içindeki gömülü sistemler üzerinde gerçekleştirilir. Bilişim teknolojilerinin günümüzdeki durumunda, bilişim sistemlerinin üzerinde çok farklı hak sahiplikleri bulunabilir. Örneğin bir web sunucunun mülkiyeti, veri merkezini işleten ve merkezdeki sunucuların genel bakımı ile işletim sistemi ve sair genel yapısını güncelleyen/işler kılan X şirketine, sunucuyu sanal olarak kullanma hakkı aracı hosting firması Y’ye, sunucunun sanallaştırılmış içeriğindeki ayrık bölümlerde veri depolama ve bu verilere erişme/değişiklik yapma hakkı ise hosting hizmeti alan müşterilere(Z) ait olabilir. Müşteri boyutunda da farklı hak sahiplikleri mevcut olabilir. Web sitesinin işlemesinde kullanılan pek çok uygulamanın da pekala hak sahiplikleri üçüncü kişilerde bulunabilir ve bu konularda siteyi işletenler ayrı bir BT firmasından hizmet alıyor olabilirler. Tüm bu unsurlar

[296] Murat Volkan DÜLGER 2022, age. s. 266.
[297] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 958, 959; Berrin AKBULUT 2017, age. s. 121.
[298] Cengiz APAYDIN 2017, age. s. 54.
[299] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 235.

bilişim sistemi içerisindeki verileri oluşturur ve bu verilerin web sunucuda bulunması, hosting sözleşmesine bağlı bir barındırma hakkının sonucudur.[300]

Web sunucuda salt yukarıda örneklendirilen tek bir web sitesine dair veri tabanı ve uygulama yazılımlarının barındırıldığı bir ihtimalde,[301] veri merkezine giren bir kişi sunucunun portuna bağlanır ve brute force saldırısı ile şifreleri kırarak ilgili bölümlere erişir ise burada (*tüzel kişilerin mağdur sıfatı kabul ediliyor ise*)[302] X, Y, ve Z'nin ayrı ayrı mağdur sıfatları doğacaktır.[303] Ancak suçun korumayı amaçladığı değerler arasında sisteme dair yalın mülkiyet hakkı bulunmadığından, örnekteki X şirketi sadece sunucuların mülkiyetine sahip olsa ve bu sunucuları fiziki olarak Y'ye kiralasaydı ve Y de fiziki sunucuları kendi işyerinde çalıştırarak sunucunun somut ve soyut alanına dair tek yetkili olsaydı, bu durumda işlenen yetkisiz erişim suçu dolayısıyla X'in mağdur sıfatına sahip olması mümkün olmayacak, suçtan zarar gören konumunda bulunabilecekti.

Başka bir örnekte ise eski sevgilisinin telefonuna yüklediği spyware üzerinden Facebook şifresini çalan fail, şifresini çaldığı Facebook hesabına yetkisiz olarak erişim sağlayabilir. Bu durumda failin gördüğü kullanıcı ara yüzü, Facebook'un veri merkezindeki sunucularında barındırılan verilerden oluşan bir siber uzaydır. Temelde ise kendi istemci bilişim sistemi üzerinden fail, Facebook'un sunucular ağına yetkisiz olarak erişmiştir. Bu örnekte kullanıcı ara yüzüne dair siber uzaya erişme ve burada işlem yapma yetkisinin bir kısmı eski sevgiliye, bir kısmı ise Facebook'a aittir. Yine eski sevgili, Facebook üyesi olmasından kaynaklı olarak sunucuda ''barındırma hakkı'' sahibidir. Böyle bir durumda da (*tüzel kişilerin mağdur sıfatı kabul ediliyor ise*)[304] hem eski sevgili hem de Facebook'un mağdur sıfatları doğacaktır.

---

[300] Bu hak çeşitli durumlara göre barındırmaya ek olarak, verileri ara yüzden değiştirme hakkını da kapsayabilir. Örneğin bulut sunucudan 100 GB alan ve buna dair IP-port bağlantılarını kiralayan aracı hosting firması, müşterisi ile arasındaki sözleşmeye bağlı olarak verileri müşterisinden izinsiz olarak değiştirmeyeceğini ve sadece barındıracağını taahhüt etmiş olabilir.

[301] Tek bir sunucu içerisinde yüzlerce ayrı bölüm, binlerce farklı kişiye verilerini barındırması için kiralanabileceğinden, sunucuya yetkisiz erişim durumunda müşteriler açısından çoklu mağduriyetler de gerçekleşebilir.

[302] Tüzel kişilerin mağdur sıfatına sahip olabilecekleri kabul edilmiyor ise örnekteki tüzel kişiler, gerçek kişiler ile değiştirildiğinde aynı sonuca ulaşılacaktır.

[303] Yargıtay bir kararında, TCK md. 244'ün tipikliği içerisinde kalan ''sisteme yetkisiz olarak veri yerleştirme'' faaliyeti neticesinde işlenen suçta, bilişim sistemlerinin sahibi olan banka tüzel kişiliğinin ne mağdur ne de suçtan zarar gören sıfatına sahip olamayacağını zira ortada banka yönünden herhangi bir zararın söz konusu olmadığını belirtmiştir. Bkz. Yargıtay 8.CD 2017/21187 E. 2017/13485 K. Bankanın hak sahipliğine konu bir bilişim sistemine yetkisiz olarak erişmek ve yetkisiz olarak sisteme veri yerleştirmek durumunda bankanın bilişim sisteminin dokunulmazlığına dair hakkının doğrudan ve ilk elden zarar gördüğünü düşündüğümüzden, bu karara katılmıyoruz.

[304] Tüzel kişilerin mağdur sıfatına sahip olabilecekleri kabul edilmiyor ise örnekteki tüzel kişiler, gerçek kişiler ile değiştirildiğinde aynı sonuca ulaşılacaktır.

Burada verilebilecek bir diğer örnek ise aracı hizmet sağlayıcıların işlettiği e-ticaret sitelerinde mallarını satan hizmet sağlayıcı firmalardır. Bu firmalar aracı hizmet sağlayıcı İSS'lere belirli bedeller ödeyerek kendi mallarını internet sitelerinde satışa sunmakta ve buna dair verilerini de aracı hizmet sağlayıcının sitesini barındıran sunucularda otomatik olarak barındırmaktadır. Bu kişiler veriler üzerindeki ''barındırma hakkının'' sahipleridirler ve bu yüzden de yetkisiz erişim suçunda diğer hak sahipleriyle birlikte mağdur sıfatına sahip olabilirler.

Dikkat edilir ise yukarıdaki örneklerde sunucularda barındırılan veriler, ''veri barındırmaya'' dair bir hakkın tecellisidir. Bu sebeple ilk örnekte Y firmasının müşterisi olarak sunucuda barındırılan siteyi işleten şirketin, site içeriğindeki pek az verinin fikri mülkiyetine sahip olabileceği unutulmamalıdır. Aynı şekilde birden fazla veri tabanının bulundurulduğu sunucu üzerindeki veri tabanlarından birinde şirketin sözleşmelerinin bulunabileceği ve sözleşmelerdeki kişisel veriler üzerinde de şirketin hiçbir hak sahibi olmayacağı akılda tutulmalıdır. Fikri hakların ya da kişisel verilere dair kişilik haklarının sahibi olan sair çok sayıdaki üçüncü kişinin ise bu suç nazarında mağdur sıfatları doğamaz. Zira bu üçüncü kişiler bilişim sisteminde barındırılan veriler(*dolaylı olarak bilişim sistemleri*) üzerinde hiçbir hak sahibi değildir. Veriler(*dolaylı olarak bilişim sistemleri*) üzerinde hak sahibi olan, siteyi işleten şirkettir ve şirket bu verileri silmekte ya da başka sunuculara taşımakta tamamen özgürdür. Bu üçüncü kişiler yalnızca verilerin bilişim verisi boyutundan ayrık olan ''bilgi'' boyutuna dair hak sahibidirler. Siteyi işleten şirket ancak bu bilgiler konusunda üçüncü kişi hak sahiplerinin haklarına riayet etmek ve örneğin bilgileri ifşa etmemek, satmamak ya da üyesiyle arasındaki sözleşme gereğince üye bölümündeki fiyat ve sair bilgileri değiştirmemekle yükümlüdür. Örneğin müşteriler banka sunucularındaki bilişim verilerinin değil, mevduatlarının hak sahibidir. Bu kişilerin ne kadar mevduatı olduğuna dair bilgilerin öğrenilmesi ise yetkisiz erişim suçunun tipikliğine konu bir netice değildir. Yine veri tabanındaki bir belgede yer alan TC kimlik bilgisinin öğrenilmesi, bunlara dair kişilik hakkı sahiplerine yetkisiz erişim suçu yönünden mağdur sıfatı kazandırmayacaktır. Ayrıca yetkisiz erişim suçu ile kişisel veriler ya da fikri-sınai mülkiyet konusu olan hususlara dair değerler de korunmamaktadır. Bu tür neticelerde içtima durumu değerlendirilmeli, gerekiyorsa ''bilgileri'' öğrenilen kişiler ancak oluşacak sair suçların mağduru sayılmalıdır.[305]

[305] Doktrinde de veriler ile ilgisi bulunanların bu suçun mağduru olamayacağı ve TCK md. 136 gibi spesifik suçların mağduru olabilecekleri yönünde görüşler mevcuttur. İçerisindeki veriler olmadan bir

Öyleyse yetkisiz erişim suçunda mağdur sıfatı ancak verileri barındırma, değiştirme, kullanma yahut sair şekillerde bilişim sisteminin ‘’soyut unsurunu da kapsayacak‘’ yetkili olma durumuna dair hak ve bu haktan doğan sistemin somut **ve** soyut unsurlarının dokunulmazlığının yetkisiz kişilerce ihlal edilmesinden kaynaklanabilir.

3.2.1.2.2. Tüzel Kişilerin Mağdur Sıfatı

Hem haksızlık hem oluşan zararın yoğunluğu ve hem de saldırıların gerçekleşme sayıları bakımından, tüzel kişilerin kullanımındaki bilişim sistemlerine(*SCADA sistemleri-finans kuruluşlarının, haberleşme altyapılarını işleten şirketlerin ve sair şirketlerin veri tabanları-devlet kurumlarının sistemleri vb*.) yönelen saldırılar daha fazladır.[306] Bu tür tüzel kişiler her türlü siber güvenlik önlemini almalarına rağmen bilişim suçlarından zarar görebildiğinden, tüzel kişilere yönelen saldırıların daha şiddetli ve faillerin de daha usta suçlular olduklarını söylemek mümkündür. Öyleyse tüzel kişilerin bilişim suçları yönünden mağdur sıfatlarının ciddiyetle üzerinde durulması gerekmektedir.

Doktrinde yetkisiz erişim suçunun mağdurunun tüzel kişiler olabileceği yönünde görüşler mevcuttur.[307] Yine genel olarak tüzel kişilerin suçlarda mağdur olabileceği yönünde görüşler de bulunmaktadır.[308] Pozitif ceza hukukumuzda mağdurun tanımı yapılmadığı gibi mağdur sıfatına dair spesifik nitelendirmeler de yoktur. Mağdurun, suç normu ile korunan ve suçun işlenmesi ile zarar gören hukuksal değerlerin sahibi olduğu ve pozitif hukukta da mağdur sıfatı için duygusal bir üzüntü duyma yahut insan olma şartı aranmadığı için fail sıfatının aksine mağdur sıfatının, hukuken hak sahibi olabilen tüzel kişilerde de bulunabilmesi gerekir.[309]

---

aletin bilişim sistemi olması imkansız olduğu ve bilgisayarın açma tuşuna basıldığı anda veriler işlenmeye başlayacağı için bu görüşlerde kastedilen, sanıyoruz ki verilerin anlamlandırılmış boyutu olan ‘’bilgi‘’ yani telefonun SD kartındaki Whatsapp sohbet kayıtlarına dair mesajlardır ve şahsi görüşlerimiz ile paraleldir. İlgili görüşler için bkz. Berrin AKBULUT 2017, age. s. 122 ve Uğur İHTİYAROĞLU 2020, age. s. 415.

[306] Bahattin ALACA 2008, age. s. 52, 53, 54.

[307] Doğan SOYASLAN 2020b, age. s. 662; Uğur İHTİYAROĞLU 2020, age. s. 415; Yavuz ERDOĞAN 2010, age. s. 1394; Meral EKİCİ ŞAHİN ve Irmak KORUCULU 2019, age. s. 596.

[308] Nevzat TOROSLU ve Haluk TOROSLU 2021, age. s. 116; Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 727, 728; Mustafa ÖZEN (2017), *Ceza Hukuku Genel Hükümler Dersleri*, Adalet, Ankara, s. 240, 241.

[309] Yalnızca gerçek kişilerin suçun mağduru olabileceğine dair görüşler için bkz. Murat Volkan DÜLGER (2021), *Ceza Hukuku Genel Hükümler*, Hukuk Akademisi, İstanbul, s. 379; Bahri ÖZTÜRK ve Mustafa Ruhan ERDEM (2021), *Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku*, Seçkin, Ankara, s. 199; Berrin AKBULUT (2018), *Ceza Hukuku Genel Hükümler*, Beşinci Basım, Adalet,

3.2.1.3. Suçun Konusu

Yetkisiz erişim suçunun konusu, bilişim sistemidir.[310] Tezin ikinci bölümünde bilişim sistemi kavramı teknik ve hukuki yönleriyle ortaya konulmuş, bu konuda benimsenen şahsi görüşler aktarılmıştır. Yine aynı bölümde yer alan alt başlıklarda, TCK bağlamında bilişim sistemi olarak nitelendirilebilecek teknolojik aletlerin hangi şartları taşıması gerektiğine dair doktrin ve yargı kararları açıklanmıştır. Bu doktrin görüşleri ve yargı kararlarından ortaya çıkan temel sonuç; yetkisiz erişim suçunun konusu bilişim sistemi olmakla birlikte, TCK bağlamında geçerli olacak bir bilişim sistemi kavramına verilen anlamların farklı olduğu ve bu sebeple suçun konusunun ifade ettiği somut karşılığın da sübjektif görüşlere göre değişmesinin kaçınılmazlığıdır.

Doktrinde hangi teknolojik aletlerin TCK bağlamında bilişim sistemi olarak kabul edileceği ve yetkisiz erişim suçunun konusunu oluşturabileceği noktasında, soruşturma ve kovuşturma aşamalarında bilirkişiye başvurulması gerektiği ve teknik konunun bu şekilde aşılmasının mümkün olacağı zikredilmektedir.[311] Lakin yukarıda da vurgulandığı üzere ne doktrinde ne de içtihatlarda, TCK bağlamında bilişim sistemi olarak kabul edilecek teknolojik aletlerin asgari hangi yeteneklere sahip olması gerektiğine dair bir görüş birliği yoktur.

Bu konuda benimsenen şahsi görüş, konunun teknik yönü bunu gerektirdiği ve ASS yahut TCK'da aksi yönde bir bilgi yer almadığından, asgari olarak verileri otomatik olarak işleme **ve** depolama özelliğine sahip olan teknolojik aletlerin, hukuken ve TCK bağlamında da bilişim sistemi sayılmaları gerektiğidir. Asgari olarak bu özelliklere sahip bilişim sistemlerinin yetkisiz erişim suçunun konusu olabilmesi için salt bu yeteneklere sahip olmaları yeterli olup, ayrıca şifreleme dahil herhangi bir siber güvenlik önlemi ile yetkisiz erişimlere karşı korunuyor olmasına gerek yoktur. Sistemlerin hukuken yetkisiz bir şekilde erişilebilmeye müsait olması, suçun konusu bağlamında yeterlidir.[312] Örneğin yeni çıkan bir tableti tanıtmak amacıyla işlek bir

---

Ankara, s. 374, 375; İzzet ÖZGENÇ (2021), *Türk Ceza Hukuku Genel Hükümler*, Onyedinci Basım, Seçkin, Ankara, s. 224; Hakan HAKERİ (2021), *Ceza Hukuku Genel Hükümler*, Adalet, Ankara, s. 118.

[310] Murat Volkan DÜLGER 2022, age. s. 267; Mehmet Bedii KAYA 2019, age. s. 222; Şaban Cankat TAŞKIN 2008, age. s. 28; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 235; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1150; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 897; Berrin AKBULUT 2017, age. s. 122.

[311] Uğur İHTİYAROĞLU 2020, age. s. 416; Özge APİŞ (2018), ''Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri'', *Yasama Dergisi*, S. 37, ss. 49-86, s. 55.

[312] Büşra ÖZÇELİK 2019, age. s. 53; Tunç DEMİRCAN 2007, age. s. 87; İbrahim ŞAHBAZ 2020, age. s. 3128; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 239;

caddedeki sütun üzerine sabitleyen ve tableti sokakta öylece bırakarak herhangi bir kişinin tableti incelemesine ve içeriğindeki verilere sınırsızca erişmesine izin vererek tanıtım yapan bir firmanın durumunda, böyle bir bilişim sisteminin hırsızlık ve sair suçların konusu olabilmesi mümkün ise de yetkisiz erişim suçunun konusunu oluşturması mümkün değildir.

Doktrinde suçun konusunun bilişim sistemi içerisindeki veriler ve siber uzay olduğu, donanım içerisinde veri yoksa suçun konusunu teşkil etmeyeceği yönünde görüşler mevcuttur.[313] Bilişim sistemi donanım + siber uzay/verilerin ayrılmaz bütünlüğünden oluşur ve zaten içeriğinde işlenecek hiçbir veri bulunmayan aletler, ışığı açıp kapatılan bir lambadan ya da elektrikli testereden farksız olacaktır. Öyleyse içeriğinde hiçbir işlemci-depolama ünitesi ve bunların ayrılmaz parçası olan verileri barındırmayan cihazlar bilişim sistemi sayılmayacaktır. Bu sebeple ilgili görüşlere katılıyoruz. Yetkisiz erişim suçunun konusu salt veriler ya da donanımlar değil, bunların ayrılmaz bütünlüğü olan bilişim sistemleridir.

3.2.1.3.1. Suçun Konusu Özelinde Gerçekleşen Hafifletici Sebep (*243/2*)

TCK md. 243/2'de, yetkisiz erişim suçunun ilk fıkradaki temel hali kastedilerek, ''*Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir*'' denilmiş ve bu şekilde suçun konusunun bedeli karşılığı yararlanılabilen sistemler olması durumuna bağlı bir hafifletici sebep yaratılmıştır.[314] Doktrinde haklı olarak ''bedeli karşılığı yararlanılabilen sistem'' kavramının yoruma açık olduğu belirtilmektedir.[315] Gerçekten de normun bu şekilde düzenlenmiş olması, doktrinde bedelin ne olması gerektiği konusunda çok farklı görüşlerin doğmasına sebep olmuştur. Hafifletici sebepte zikredilen ''sistemler'' kavramının özünde bilişim sistemi olduğu izahtan vareste ise de hangi sistemin bedeli karşılığında yararlandırılıyor sayılacağı konusunda da ''*neyin bilişim sistemi kabul edileceği*'' noktasındaki farklı görüşlerden dolayı, bu hususta da farklı yorumlar ortaya çıkmıştır.

Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 900, 901, 902; Abdulrahman Hussein KAREEM 2019, age. s. 36; Berrin AKBULUT 2017, age. s. 132, 133, 134, 135 / Aksi yönde ve katılmadığımız görüşler için bkz. Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 960.

[313] İbrahim ŞAHBAZ 2020, age. s. 3127; Ramazan DOĞAN 2014, age. s. 51, 52.

[314] Ali KARAGÜLMEZ 2014, age. s. 208.

[315] Age. s. 208; Murat Volkan DÜLGER 2022, age. s. 279; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1154.

Evvela doktrinde bedel kavramına verilen farklı yorumlara değinmek gerekirse, bir görüşe göre normda zikredilen bedelin salt para verilmesine dair bir bedel olması gerekmez.[316] Aynı yöndeki diğer bir görüşe göre bedelin bir hizmet ve örneğin makale gönderimi ya da ponzi sistemlerdeki gibi üye/takipçi getirilmesi olması mümkündür.[317] Üçüncü olarak, form ya da anket doldurularak erişilebilen internet ortamlarının da bu noktada değerlendirilmesi gerektiği belirtilmektedir.[318] Dördüncü bir görüş ise bunlara ek olarak ‘’işlemci gücünün paylaşılması‘’ şartı getiren madencilik uygulamalarını örnek vererek, bu eylemin de bedel kavramına dahil olduğunu belirtmektedir.[319] Doktrinde zıt yönde bulunan görüşler ise bedel kavramını parasal ücretlendirmeler ile açıklamaktadırlar.[320]

İkinci olarak bedeli karşılığında kullandırılan bilişim sistemlerinin ne olduğu noktasında doktrinde ayrık görüşler mevcut olup, ayrımın temelinde internet kafeler yer almaktadır. Doktrinde genel olarak ücreti karşılığı kullanılabilen uygulamalar, Netflix ya da Kazancı gibi ücreti karşılığı kullanılabilen veri tabanları ve ağ bağlantısı üzerinden erişilen sair ortamlar ‘’bedeli karşılığı yararlanılan sistem‘’ kavramı içerisinde kabul edilmektedir.[321]

İnternet-Playstation kafelerdeki ya da bilişim sistemlerini bedeli karşılığında kullandıran sair noktalardaki sistemlerden bedelsiz yararlanmayı hafifletici sebep içerisinde değerlendirmeyen görüşlerin dayandığı temel husus, bedelsiz olarak yararlanılması gereken yapının siber uzayda sunulan hizmetler olduğudur.[322] Biz bu görüşlere katılmıyoruz. Zira bilişim sistemi kavramı donanım + siber uzayın ayrılmaz bütünlüğüdür. İnternet kafe ve sair işletmelerde de bilişim sistemleri kullandırılırken, kapalı bilgisayarın tuşlarına basılması gibi salt donanımlarının kullanılmasına yönelik amaçlarla bedel ödenmediğinden, bedel karşılığı sistemin kullanılması ile erişilen yer

[316] Yavuz ERDOĞAN 2010, age. s. 1397; Murat Volkan DÜLGER 2022, age. s. 280; İbrahim ŞAHBAZ 2020, age. s. 3133.
[317] Ali KARAGÜLMEZ 2014, age. s. 210; Ali PARLAR ve Mustafa ÖZTÜRK 2020, age. s. 31; Tunç DEMİRCAN 2007, age. s. 97; Özge APİŞ 2018, age. s. 60.
[318] Damla ERMEYDAN (2018), *Türk Ceza Kanunu'nda Bilişim Suçları*, Çağ Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Mersin, s. 63.
[319] Kaya, Hukuki Açıdan Bilişim Suçları, s. 227.
[320] Cengiz APAYDIN 2017, age, s. 63; Ali PARLAR ve Mustafa ÖZTÜRK 2020, age. s. 31; Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2012, age. s. 445.
[321] Ahmet Caner YENİDÜNYA 2005, age. s. 13; Berrin AKBULUT 2017, age. s. 147; Burak ÇEKİÇ 2006, age. s. 98; Murat Volkan DÜLGER 2022, age. s. 280.
[322] Nagihan GÜN 2020, age. s. 199, 200; Ali PARLAR ve Muzaffer HATİPOĞLU 2010, age. s. 3746; Ali KARAGÜLMEZ 2014, age. s. 210.

her halükarda siber uzaydır. Öyleyse internet kafelerdeki hizmetin de hafifletici sebebe konu olacağı yönündeki sair görüşlere[323] katılmak gerekir.

Hafifletici sebep nazarında değerlendirilebilecek ‘’bedeli karşılığı yararlandırılan‘’ bilişim sistemleri arasından, sistemlerin fiziksel olarak kullandırıldığı örnekler salt internet-Playstation kafeler veya sanal gerçeklik teknolojilerini ücret karşılığı kullandıran benzer işletmeler değildir. Bir kütüphanenin, salonlarında bulunan bilgisayarlarını kullandırarak bu bilgisayarlar üzerinden arşivlere erişim hizmeti vermesi ve bu hizmeti de bir ücret karşılığında sunması mümkündür ve bu gibi durumlar da TCK md. 243/2 nazarında değerlendirilmelidir.

Bir sistemin arada bir gelir elde etmek için ücretlendirilmesi ve örneğin bir kişinin bilgisayarını komşusuna bazen ücretli kullandırması, öğrencinin ücreti karşılığı arkadaşlarına hotspot internet bağlantısı açması, ücreti karşılığı zaman zaman bir online oyun hesabının şifresinin üçüncü kişilere verilmesi ve onların da hesaptaki karakter üzerinden oynamalarının sağlanması gibi durumlarda ise ‘’bedel karşılığı hizmete özgüleme‘’ durumu olmadığından, bu tür durumlar hafifletici sebebin konusunu oluşturmaz.

TCK md. 243/2’nin lafzında ‘’*bedeli karşılığı yararlanılabilen*‘’ denildiğinden, bedeli karşılığında mülkiyeti satılan bilişim sistemleri de hafifletici sebebin konusunu oluşturmaz. Zaten bu tür durumlar ve örneğin teknoloji mağazasında satılan bir bilgisayarın bedeli ödenmeden alınıp götürülmesi ve kullanılması, hırsızlık suçunun objektif tipikliği içerisinde kalacaktır. Aynı şekilde içerisinde müzikler olan bir USB’nin kiralanması ya da fiziki sunucunun aracı hosting firmasına verilmesi gibi durumlarda bunlar kira ilişkisi olmaksızın alınır ise hırsızlık, kira ilişkisi sona ermesine rağmen geri verilmeden bedelsiz kullanım gerçekleşir ise güveni kötüye kullanma suçları gündeme gelecektir.

Bedeli karşılığında yararlanılabilen bilişim sistemleri noktasında önem arz eden bir diğer konu da bedelsiz olarak yararlanılanın bilişim sistemi olması gerektiği, bu sebeple salt verilerin ve örneğin bir yazılımın bedelsiz kullanımının TCK md. 243/2 nazarında değerlendirilemeyeceğidir. Örneğin X internet bağlantısı ile okunabilen günlük gazeteye dair mobil uygulama, Y ise içerisinde bir sürü kitap yüklü şekilde indirilen bir e-kitap uygulaması olsun. Bu iki uygulama da ücret karşılığında bilgisayara indirilebiliyor olmasına rağmen bir şekilde ücret ödenmeden indirilir ise

[323] Ahmet Caner YENİDÜNYA 2005, age. s. 13; Esra YAYCI 2007, age. s. 82, 83.

bilgisayara her iki uygulamanın da veri dosyaları yüklenmiş olacaktır. Her iki uygulama da bu indirilen veri dosyaları üzerinden bir noktaya kadar bedelsiz olarak kullanılabilir. Bu durumda X uygulamasında ‘’şifrenizi giriniz‘’ bölümüne kadar, Y uygulamasında ise içerisindeki her noktaya kadar bedelsiz kullanımda bulunulması mümkün olacaktır. Salt verilerden oluşan bu yazılımların bedelsiz olarak kullanımı ancak fikri mülkiyete dair suçlar yönünden gündeme gelebilecektir. Lakin X uygulaması günlük bir gazetenin okunması olduğundan ve bu okuma da günlük gazetenin verilerinin yüklendiği web sunuculara internet üzerinden bağlantı sağlanması vasıtasıyla yapılabileceğinden, uygulama bedelsiz indirildikten sonra ayrıca gazete bedelsiz olarak okunur ise burada bedeli karşılığı yararlanılabilen bir bilişim sistemine yetkisiz olarak erişim gerçekleşecektir. İşte salt yazılımların değil ancak bilişim sistemlerinin içeriğine yetkisiz olarak erişildiği bu gibi durumlar TCK md. 243/2 nazarında değerlendirilebilirler.

Bedeli karşılığı yararlandırılan bir bilişim sistemine yetkisiz erişimin söz konusu olduğu bir olayı konu eden ve TCK md. 243/2 noktasında son derece faydalı bir örnek oluşturan aşağıdaki Yargıtay içtihadının burada paylaşılması yararlı olacaktır. Kararın ilgili kısmı şöyledir:

> ‘’*… Sanık ...'nin nun ... Esnaf ve Sanatkârlar Odası başkanı, diğer sanıkların de odanın bilgi işlem kısmında çalışan elemanları oldukları, sanıkların ... Esnaf ve sanatkarlar odası üyelerine ait ellerindeki bilgilerin doğruluğunu teyit etmek istedikleri, bunun için Nüfus ve Vatandaşlık İşler Genel Müdürlüğü ile anlaşma yapıp* ***ücreti karşılığı yararlanmak yerine****, bunu haksız şekilde yapmayı planladıkları, bunun için www.isimtescil.net bilişim sistemi ara yüzünden Mernis sistemindeki kimlik bilgilerini karşılıksız çekmek için bir yazılım hazırladıkları, bu düzeneği ... Esnaf ve sanatkarlar odasına ait bina içindeki sunucu üzerinde çalıştırıp milyonlarca sorgu gönderip Mernis'te kayıtlı verileri sürekli şekilde çektikleri, …*‘’.[324]

Görüldüğü üzere olayda ücretli olarak erişilen Mernis veri tabanına ücretsiz/bedeli ödenmeden erişilmiş ve içeriğindeki veriler elde edilmiştir. Bu durum TCK md. 243/2 yönünden son derece somut bir örnektir. Lakin kararda olaya dair 244. maddenin tatbik edilmesi gerektiği belirtilmekte olup, bu sebeple karar kanaatimizce hatalıdır.[325]

---

[324] Yargıtay 15. CD 2017/14178 E. 2020/4067 K.

[325] Yargılamaya konu olayda 244. maddenin unsurları oluştuğu düşünülüyorsa, kanaatimizce bu durum içtima noktasında ayrıca değerlendirilmeliydi. Zira kararın lafzından açıkça görüldüğü üzere bilişim sistemine girme/yetkisiz erişim suçunun TCK md. 243/2’de düzenlenen hafifletici sebebinin unsurlarının oluştuğu net biçimde görülmektedir.

3.2.1.3.1.1. Bedel Kavramına Dair Değerlendirme

Yalnızca yetkililerin erişebildiği sistemler; kamunun erişimine kapalı, belirli kişilerin bedelsiz olarak veya bedelini ödeyerek erişilebildiği sanal ortamlarıdır. Bu noktada yetkilendirilmeyi ikiye ayırmak mümkündür. Evvela yetkilendirme ihtiyacı duyulan sistemlerin bir kısmında bu yetkiler, kullanıcıların sübjektif özelliklerine göre verilir ve örneğin bir kişi her arkadaşına değil, sadece canının istediklerine ve karşılık beklemeksizin yetki verir. Aynı şekilde bir şirketin, bilgisayar mühendisliği diplomasını sunan herkese sistemlerini kullandırması gibi bir zorunluluğu bulunamayacağından, şirket sübjektif seçimleri dahilinde işe aldığı çalışanlarından yine şahsi istekleri doğrultusunda seçtikleri arasında sistemleri dağıtmakta ve işin gereği olarak bir karşılık beklemeden kullanım izni vermektedir.

İkinci olarak, yetkililerin erişebildiği/kullanabildiği sistemlerden kimilerinde ise bazı bedelleri ödeyen ve ödün veren kullanıcıların yetkilendirilmesi gerçekleşir. Bunlardan bir kısmında bedeli ödeyen her istekliye erişim izni verilmesi zorunlu değildir. Sair kısmında ise bedel ödeyen isteklilerin sübjektif özellikleri göz önünde bulundurulmaksızın, bedeli ödeyen her istekliye yetkilendirilme ve erişim izni verilir. Örneğin bir anonim ağa katılabilmek için bilgisayarın ağdaki proxy ya da p2p sunucular ağına açılmasını ve trafiğin üzerinden geçmesini şart koşan teknolojiler bulunmaktadır ve bu bedeli ödeyen herkes teknolojileri kullanabilmektedir. Aynı şekilde uygulamayı kullanabilmek için kullanıcıların sistemlerindeki verileri diğer kullanıcılara açmasını şart koşan yazılımlar da mevcuttur. Bu tür durumlarda ilgili şartlar gerçekleştirildikten sonra tıpkı içeriğine erişebilmek için bir makale gönderimini şart koşan internet sitesindeki gibi kullanıcıya yetki için şifre gönderilebileceği gibi bu yetki doğrudan sistem özellikleri noktasında da verilebilir. Yine örneğin Instagram, üye olup uygulamanın kullanılabilmesi için fotoğraf gönderimini şart koşsaydı, fotoğraf gönderimi yetkinin satın alınması noktasında bir bedel sayılacaktı. Bedeli ödeyen herkesin genel olarak erişim yetkisi sahibi olduğu bu tür hizmetlerden bazısında ise yetkilendirmeler ücret karşılığı yapılır ve örneğin aylık ödenen bir para karşılığı kütüphane veri tabanına üyelik şifresi alınır, alınan şifre ile kütüphanedeki bilgisayarlardan veya uzaktan sunuculara bağlanılarak arşivlere erişilebilir.

Kanaatimizce TCK md. 243/2'de yer alan bedel kavramının, yalnızca parasal ve maddi bir karşılık olarak anlaşılması gerekmektedir. Bu sebeple ilgili normun kapsamına yalnızca ''bedeli karşılığında ve üyelik/yönetici onayı sonrası erişilebilen,

sistem yöneticilerinin siber güvenlik kaygıları haricinde müşterilerin kişisel özelliklerini dikkate almaksızın bedelini ödeyen her isteklinin talebine onay verdiği, bedel karşılığı yararlandırılan bu hizmetin de müşteriler yönünden bir tüketici ilişkisi yarattığı hizmetler'' girebilir. Bu hizmetlerin ise internet ağından bağlanılarak, LAN üzerindeki intranetlerde yahut fiziki olarak başına oturan bilgisayarın kullanılmasıyla ve sair şekillerde yapılması mümkündür. Burada önemsenmesi gereken temel husus, bedeli karşılığı hizmet verenlerin keyfi olarak isteklilere karşı ''sistemden yararlandırmıyorum'' diyememeleri ve bunun tüketici hukuku nazarında bir hukuksuzluk yaratacak olmasıdır. Aksi takdirde hafifletici sebebin uygulanabilmesinde bir standardizasyonun sağlanması mümkün olmayacağı gibi bedelin yalnızca para olmadığı görüşü kabul edilirse, son derece sakıncalı hukuki durumlar doğabilir. Zira doktrindeki örnekler genel olarak bedele dair ''makale gönderimi ya da başka üyeler de getirme'' gibi internette örnekleri bulunan uygulamalara yönelik verilmiş ise de bir kişinin kendisiyle akşam yemeğine çıkmayı, amuda kalkmayı ve sair durumları bedel olarak belirlediği hizmetler de teorik açıdan aynı durumu ifade edecektir. Bu sakıncalı yoruma göre yetkili erişim gerektiren bilişim sistemlerinin büyük bir çoğunluğu hafifletici sebebe dahil edilebilir ve örneğin sadece arkadaşı olanları sisteminden yararlandıran bir kişinin durumunda ''arkadaş olmak'' dahi bir bedel kabul edilebilir. Bu da şüphesiz ki normun ruhuna uygun değildir.

3.2.1.3.1.2. Daha Düşük Cezanın Temel Gerekçesi

Kanun koyucunun TCK md. 243/2'deki norm ile bir hafifletici sebep düzenlemesi yaratması ve bunu bedeli karşılığı yararlanılan sistemler üzerinden yapması, bu durumda kanun koyucunun normun korumayı amaçladığı değerlere tecavüz eden haksızlığın daha az olduğunu düşündüğünü göstermektedir. Tüketici-sağlayıcı ilişkisinin bulunduğu hizmetlerde bedelini ödeyen herkesin hizmetten faydalanması mümkün olduğundan, bu tür durumlarda bilişim sistemlerine kamunun erişim olanağına dair kısmi bir açıklık bulunur. Bu sebeple bu tür hizmetlere özgülenmiş sistemlerin dokunulmazlığı olgusu, diğerlerine göre daha az yoğunluktadır.[326] Örneğin bir yanda Radyo, Televizyon ve İsteğe Bağlı Yayınların

[326] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 904; Ahmet Caner YENİDÜNYA 2005, age. s. 13; Ali KARAGÜLMEZ 2014, age. s. 211; Cengiz APAYDIN 2017, age. s. 66, 67; Hayati PALLI 2008, age. s. 154; Hasan Burak ÖNDİN 2017, age. s. 39; Meral EKİCİ ŞAHİN ve Irmak KORUCULU 2019, age. s. 615.

İnternet Ortamından Sunumu Hakkında Yönetmelik'te detaylandırılan platform işletmeciliği ve medya hizmet sağlayıcılığı hizmetlerinin bedeli karşılığında verilen türleri diğer yanda ise bir şirketin, çalışanlarının salt işyerinde erişebilmesi için hazırladığı bir intranet film-müzik veri tabanı bulunsun. Platform işletmecisinin platformunda yer alan veri tabanına bedelini ödeyen herkes erişebiliyorken, şirketin intranet veri tabanına hangi bedeli öderse ödesin dışarıdan kimse erişememektedir. İki sisteme de yetkisiz olarak erişildiğinde, bu durumda suçların haksızlık içeriğinde bir fark olacağını düşünen kanun koyucu, bu konuda standart yaratabilmek için TCK md. 243/2'de bir hafifletici sebep oluşturmuştur.

Sistemlerin erişilebilirliği üzerinden yapılan bu hafifletici sebep doktrinde eleştirilmekte[327] ve bazı görüşler bu durumlarda cezanın indirilmek yerine artırılması gerektiğini belirtmektedir.[328] Bedelini ödeyen herkesin erişebildiği bilişim sistemleri ile sair sistemler arasında TCK md. 243/1 bağlamında gerçekten de haksızlık derecesi bakımından fark bulunmaktadır ve bu sebeple cezanın artırılması gerektiği yönündeki görüşlere katılmak mümkün değildir. Lakin biz de mevcut haliyle TCK md. 243/2'deki hafifletici sebebin doğru olmadığını, normun daha ayrıntılı bir yapıya kavuşturulması gerektiğini düşünüyoruz. Zira normda evvela bedeli karşılığı yararlandırılan sisteme ne şekilde bedelsiz erişildiği zaman cezanın hafifleyeceğine dair bir ayrıntı yoktur. Bedeli karşılığı kullanıma sunulan Netflix veri tabanı örneğinde, başka bir Netflix üyesinin giriş bilgileri ile bu bedelsiz/yetkisiz erişim sağlanabileceği gibi Netflix'in yazılımları aşılarak da uygulama üzerinden bu erişim gerçekleşebilir. Fakat veri tabanının barındırıldığı sunucular ağına veya ağdaki bir bölüme Netflix'in kullanıcılarına sunduğu uygulama yazılımı aracı kılınmaksızın da erişilebilir ve bu yöntemler çok ciddi hacking saldırılarını teşkil edebilir. Netflix uygulaması üzerindeki açıklıklar keşfedilerek uygulama üzerinden veya sunucu tarafındaki açıklıklar keşfedilerek sair yollardan yapılan bir kısım yetkisiz erişimler ve buna yönelik hacking faaliyetleri Netflix'in açığını kapamasına yarayabilecek olsa da tüketici ilişkileri, kişisel veriler, marka değeri ve açıkların giderilmesi için yapılacak giderler ciddi maddi-manevi zararlar doğurabilecektir. Bu sebeple TCK md. 243/2'nin ağ bağlantısı

[327] Berrin AKBULUT 2017, age. s. 142, 143; Yavuz ERDOĞAN 2010, age. s. 1400.
[328] Murat Volkan DÜLGER 2022, age. s. 283, 284; Büşra ÖZÇELİK 2019, age. s. 102 / Bazı görüşler ise bu hafifletici sebebin getiriliş amacının otomatların bedelsiz kullanımını düzenleyen TCK md. 163 ile cezada paralellik yaratılması isteği olduğu belirtmektedir. Bu konuda bkz. Muammer KETİZMEN 2006, age. s. 134.

yoluyla kullanıcılara verilen ücretli hizmetler yönünden, sadece şifre-kullanıcı adı ve benzeri hususta ele geçirme/brute force saldırısı sonucu ve uygulama/site üzerinden yapılan yetkisiz erişimlerde hafifletici sebep sayılması daha doğru olurdu. Aynı gerekçeyle, internet kafedeki bilgisayarın ya da kütüphanedeki bilgisayarların hacklenerek bedelsiz erişim sağlanması da hafifletici sebep sayılmamalıdır.

3.2.1.3.1.3. Normun Karşılıksız Yararlanma Suçu ile İlişkisi

TCK md. 163'te düzenlenen karşılıksız yararlanma suçunun, TCK md. 243/2'nin konusunu oluşturan bedeli karşılığı yararlanılan bilişim sistemleri ile bağlantısı mevcuttur. Karşılıksız yararlanma suçunu düzenleyen 163. maddenin üç fıkrasının birincisinde,

> ''*Otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan yararlanan*'', ikincisinde ise ''*Telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan*''

denilmekle, suçun bedeli karşılığında yararlandırılmaya tahsis edilmiş bir bilişim sistemine yetkisiz olarak erişmek suretiyle işlenebilmesinin mümkün olduğu gibi bir izlenim yaratılmıştır.

TCK md. 163'ün ''*Telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlar*'' şeklindeki ikinci fıkrasında telefon hatları ile frekanslarından karşılıksız yararlanmak ilk seçimlik hareket, elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan karşılıksız yararlanmak ise ikinci seçimlik harekettir. İlk seçimlik harekete dair bir değerlendirme yapmak gerekirse, telefon hatları ile frekanslarından karşılıksız yararlanılması, erişim sağlayıcıların omurga yapıları ve routerları üzerinden internet ağına bedelsiz erişmeyi kapsamına almaktadır. Ancak internet omurgası sadece telefon hatlarından ve frekanslarından oluşmadığından, omurganın sair kısmına yönelik TCK md. 163'ün bir bağlantısı bulunmamaktadır. Elektromanyetik dalgaların çatı bir kavram oluşu, ikinci seçimlik hareket yönünden yayına aracılık eden veri nakil araçlarının sınırlı sayıda sayılmadığını göstermektedir. Öyleyse kablosuz iletişim teknolojilerinin kullanılması suretiyle ve ağ üzerinden bilişim sistemlerinin iletişimi vasıtasıyla yapılan şifreli/şifresiz yayınlar, bu noktada normun kapsamında kalmaktadır.

TCK md. 243, bilişim sistemleri yönünden TCK md. 163/2'ye göre özel norm olduğundan, internet omurgasının(*internete erişim hizmeti*) bedelsiz kullanımı ve

istemci-sunucu/verici-alıcı iletişiminde bilişim sistemlerine erişilerek bedelsiz yararlanılan yayınlarda TCK md. 243'ün uygulanması gerekir. İşin içine bilişim sistemine erişimin girmediği durumlarda ise TCK md. 163/2'nin uygulanması doğru olacaktır.[329] Öyleyse TCK md. 163/2 ile TCK md. 243/2 arasında yapılacak seçim, bedelsiz yararlanma durumunun ''bir bilişim sistemine yetkisiz erişim'' teşkil edip etmemesine bağlıdır. Belirtmek gerekir ki internet omurgası değil televizyon vericileri ile yapılan şifreli/şifresiz yayınlarda da TCK md. 243/2'nin özel norm olarak uygulanması mümkündür. İnternet üzerinden televizyon yayını haricinde, kablolar ve uydular üzerinden gerçekleşen klasik televizyon yayıncılığı yani karasal yayın sistemi de mevcuttur. Bu yayın tiplerinde de eğer vericinin bilişim sistemi olduğu ortaya konulabiliyor ise bu durumda şifreli bir televizyon yayınının TV altyapısı üzerinden bedelsiz izlenmesi de TCK md. 243/2'nin uygulama alanında kalmalıdır.[330]

Normun birinci fıkrasında yer alan otomatların TCK'da bağlayıcı bir tanımı olmadığından her otomatın bilişim sistemi olması gerekmez ve hatta elektrik enerjisi ile çalışmayan, manuel aletlere de otomat görevi gördürülebilir. Bunun yanında teknik olarak bilişim sistemi sayılan ve çeşitli programlamalar dahilinde çalışan otomatlar da mevcuttur. Lakin TCK md. 163 ile TCK md. 243/2 arasındaki ayrımın otomatlar yönünden noksansız biçimde yapılabilmesi mümkün görünmemektedir. Zira TCK md. 163/2'de internet gibi spefisik bir ağ teknolojisi belirtilmeden suçun objektif tipikliği oluşturulmuş, 163/1'de ise direkt olarak spesifik bir alet olan otomatlar üzerinden düzenlemeye gidilmiştir. Örneğin eğer bir normda, ''*bir NAS sisteminin içerisindeki verileri değiştirmek, erişilemez kılmak ya da yok etmek ...*'' şeklinde bir suç düzenlenseydi, NAS'ın içeriğindeki veriler değiştirildiğinde bilişim sistemlerinin içeriğindeki verilerin değiştirilmesini suç olarak düzenleyen TCK md. 244/2

[329] İnternet erişiminin bedelsiz kullanılmasına dair aynı yönde bkz. Berrin AKBULUT 2017, age. s. 145 / Bilişim sistemine erişim mevcut ise şifreli yayınlara bedelsiz erişim durumunda her iki suçun da oluşacağı ve fikri içtimanın uygulanabileceği yönünde bkz. Büşra ÖZÇELİK 2019, age. s. 55, 56, 57 / TCK md. 243/2 ve 163/2'nin aynı anda oluştuğu ve içtima kurallarına göre en ağı cezayı gerektiren suçun uygulanmasına dair görüşler konusunda ayrıca bkz. Yargıtay 11. CD 2012/439 E. 2013/16403 K. İçinde, Büşra ÖZÇELİK 2019, age. s. 57 / Aksi yönde görüşler için bkz. Ahmet Caner YENİDÜNYA 2005, age. s. 13 / Aksi yönde karar için bkz. Yargıtay 13. CD 2014/34290 E. 2015/6590 K. İçinde, Büşra ÖZÇELİK 2019, age. s. 58 / Dekoderlerin salt TCK md. 163/2 içerisinde değerlendirilmesi gerektiğine yönelik aksi yöndeki görüşler için bkz. Burak Cesur AKÖZ 2018, age. s. 85; Ramazan DOĞAN 2014, age. s. 76; Hasan Burak ÖNDİN 2017, age. s. 40; Ahmet Caner YENİDÜNYA 2005, age. s. 13; Fazıl GÜRLER 2013, age. s. 102 / Şifreli yayınların külliyen TCK md. 163/2 içerisinde değerlendirilmesi gerektiğine dair aksi yönde görüşler için bkz. Hakan KARAKEHYA 2009, age. s. 10.

[330] Televizyon yayınının hazırlanışında, çağın gereği olarak bir sürü bilişim sistemi kullanılmaktadır. Bilgisayar ve sair bilişim sisteminden aldığı verileri ileten televizyon vericisi eğer bilişim sisteminin veri işleme-depolama özelliğini taşımıyorsa, bu noktada TCK md. 243/2 uygulanamaz.

uygulanmayacaktı. Zira NAS'a dair bu farazi norm, 244. maddeye göre özel norm sayılacaktı. Aynı şekilde bilişim sistemi olan otomatların da özel olarak ''otomatlar'' denilerek yapılan bir düzenlemeyi içeren TCK md. 163/1'in içerisinde değerlendirilmesi gerektiğini ve otomatlar yönünden TCK md. 163/1'in özel norm olduğunu düşünüyoruz. Doktrinde de TCK md. 243/2'de karşılıksız yararlanma suçunun konusu olan otomatların kastedilmediği,[331] karşılıksız yararlanma suçunda otomatların özel olarak düzenlendiği yönünde görüşler mevcuttur.[332]

3.2.1.4. Fiil ve Netice

Yetkisiz erişim suçunun düzenlendiği TCK md. 243/1'de ''*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden*'' denilmekle, seçimlik hareketli bir suç yaratılmıştır. Bu seçimlik hareketlerden ilki bilişim sisteminin bütününe veya bir kısmına yetkisiz olarak erişmek/girmek, diğeri ise bilişim sisteminde yetkisiz olarak kalmaya devam etmektir.[333]

Normda bu yönde bir düzenleme yer almadığından, bu seçimlik hareketlerin ne şekilde gerçekleştirildiğinin ve örneğin ağ bağlantıları vasıtasıyla ya da fiziksel yöntemlerle yapılmasının bir önemi bulunmamaktadır. Örneğin seçimlik hareketler internet ağı vasıtasıyla gerçekleştirilebileceği gibi fiziken sistem portuna bağlanılarak ya da direkt olarak sistemin başına oturulup sistem kullanılarak da gerçekleştirilebilir.[334]

Bilişim sistemine yetkisiz erişim ve bilişim sisteminde hukuka aykırı olarak kalmaya devam etmek durumları hem suçun objektif tipikliğine konu fiiller hem de oluşan durum sebebiyle suçun neticeleridir. Bu sebeple seçimlik hareketler neticesinde oluşan bu suç, neticesi hareket ile bitişik bir suçtur.[335]

---

[331] Murat Volkan DÜLGER 2022, age. s. 279.

[332] Doğan SOYASLAN 2020b, age. s. 666; Ali KARAGÜLMEZ 2014, age. s. 209; Hasan Burak ÖNDİN 2017, age. s. 40.

[333] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 232; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1151; Murat Volkan DÜLGER 2022, age. s. 246; İbrahim ŞAHBAZ 2020, age. s. 3127.

[334] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 900, 901, 902; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1150, 1151; Ahmet Caner YENİDÜNYA 2005, age. s. 9; Ahmet GÜL 2021, age. s. 98; Doğan SOYASLAN 2020b, age. s. 662, 663.

[335] Evrende gerçekleşen her durum, kanaatimizce bir eylem ve sonuç doğurur. Maddi ceza hukukunun konusu olan durumlar yönünden bu değerlendirme, suç tiplerine konu her fiilin bir neticesinin bulunacağı yani neticesiz bir suçtan söz edilemeyeceğidir. Örneğin yetkisiz erişim suçunda bir bilgisayara erişme hareketi salt fail yönünden gerçekleştirilen bir eylem olmanın ötesinde, ''bilgisayarın yetkisiz erişime maruz kalmış olması'' noktasında mağdur ve geri kalan tüm evrende yaratılan bir

Suçun birinci fıkradaki temel halinde ve ikinci fıkrada düzenlenen hafifletici sebep düzenlemesinde, objektif tipikliğin oluşumu yönünden sisteme yapılan yetkisiz erişimler sonucunda ve/veya hukuka aykırı olarak kalmaya devam edildiği sırada, sistemlere zarar verilmesi ya da sistemde yer alan verilerin öğrenilmesi objektif tipikliğin oluşumu için şart değildir.[336] Vurgulamak gerekir ki verilerin öğrenilmesi salt sistem içerisinde depolanan veri dosyalarının depolanmış hallerinin ya da verilerden oluşan anlamlı bilgilerin öğrenilmesi değildir. Verilerin işlenmesiyle çalışan yazılımların göz ya da sistemler vasıtasıyla öğrenilmesi de verilerin öğrenilmesi sayılır. Zira bir durumda depolanmış verilere dair bilgi, diğer durumda veriler işlenirken çalışan programlar yani verilerin canlı halleri görünür. Öyleyse yetkisiz erişilen hedef sistemde yer alan verilerden gelen her karşılık, örneğin yalnızca ‘’hoşgeldiniz‘’ yazısının bulunduğu bir ekran bile bu sonucu doğuracaktır. Bu sebeple suçun ‘’sistemde yer alan verilere dair bilgiler öğrenilmeden‘’ işlendiği durumlar, pratikte özellikle ağ yapılarına karşı gerçekleştirilen yetkisiz erişimlerde ortaya çıkar. Örneğin bir bluetooth ya da wi-fi ağına yetkisiz olarak erişildiğinde herhangi veriye dayalı bilgi ile bu bilgiyi öğrenebilecek düzeyde direkt olarak temasa geçilmemektedir.

Doktrinde suçun, bilişim sistemine yetkisiz olarak erişmek seçimlik hareketi yönüyle ani bir suç özelliği taşırken,[337] sistemde yetkisiz olarak kalmaya devam etmek seçimlik hareketi yönüyle mütemadi bir suç özelliği taşıdığı ve sistemde yetkisiz olarak kalmaya devam edildiği sürece suçun işlenmesi süreceğinden, sisteme erişim

---

sonuçtur. Buradaki özel durum, hareket ile netice arasına üçüncü bir bağlantının girmemesi ve neticenin harekete bitişik olmasıdır. Neticesi harekete bitişik suçlar yönünden bkz. Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 100, 101 / Yetkisiz erişim suçunu neticesi harekete bitişik bir suç olarak algılayan görüş için bkz. Doğan SOYASLAN 2020b, age. s. 662, 663. Suç tipini netice unsuruna da yer vererek inceleyen benzer görüş için bkz. Ali KARAGÜLMEZ 2014, age. s. 205 / Her suçun bir neticesi olmadığı yönündeki görüşlere göre ise neticesi harekete bitişik suçlarda bir netice bulunmaz ve bunların salt hareket suçları olarak nitelendirilmeleri gerekir. (*Bkz. Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 99*) / Yetkisiz erişim suçunun salt hareket suçu olduğu yönünde görüşler için bkz. Murat Volkan DÜLGER 2022, age. s. 268; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 900, 901, 902; Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2012, age. s. 443; Berrin AKBULUT 2017, age. s. 128.

[336] Murat Volkan DÜLGER 2022, age. s. 268, 273, 274; Ali PARLAR ve Muzaffer HATİPOĞLU 2010, age. s. 3743; Muhammet Sefa ÇETİN 2021, age. s. 5; Cengiz APAYDIN 2017, age. s. 60; Ergün, age. s. 89; Ramazan DOĞAN 2014, age. 69; Doğan SOYASLAN 2020b, age. s. 662, 663; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 900, 901, 902; Ahmet Caner YENİDÜNYA 2005, age. s. 10; Burak ÇEKİÇ 2006, age. s. 91; Hüdaverdi UÇAR (2014), *5237 s. Türk Ceza Kanunu'nda Bilişim Suçları*, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara, s. 54; Berrin AKBULUT 2017, age. s. 129, 130; Mehmet Bedii KAYA 2019, age. s. 223, 224; Ahmet GÜL 2021, age. s. 100; Uğur İHTİYAROĞLU 2020, age. s. 425; İbrahim ŞAHBAZ 2020, age. s. 3124.

[337] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 238, 239, 247.

sonlandığı an suçun tamamlanacağı belirtilmektedir.[338] Kanaatimizce bilişim sistemlerine erişmek ve kalmaya devam etmek fiilleri, suçun işlenme süreleri bakımından farksız seçimlik hareketlerdir. Zira bir sisteme erişim sağlayabilmek demek, sistemde yarım saniye bile olsa belirli bir süre kalmak demektir. Öyle ki örneğin bir evin camından içeriyi gözlemek ile camı açıp eve girmek farklı maddi durumları yansıtıyor olsa da sisteme erişmek de sistemde kalmak da ilgili örnek bakımından camı açıp içeriye girmek/içeride olmak durumunu nitelemektedir.

Bir bilişim sistemine yetkisiz olarak erişildiği an suçun objektif tipikliği oluşuyor ise de erişim kesilene kadar suçun icrası devam edecektir ve bu durum aylar sürebilir. Bu sebeple sisteme yetkisiz olarak erişen kişi otomatikman bir saniye bile sistemde yetkisiz olarak kalmaya devam ettiğinde, suçun unsurlarının oluşması/işlenmesi ile suçun işlenmesinin sonlanması arasında belirli bir süre bulunacak ve bu durum eşyanın tabiatından kaynaklandığı için iki ayrı suç ya da iki ayrı fiil gündeme gelmeyecektir.[339] Aynı şekilde bir sisteme yetkili olarak erişildikten sonra yetkisiz olarak kalmaya devam edilmesi durumunda da kalmaya devam etme süresi bir saniyelik bir süre olabileceği gibi bu durum da aylar sürebilir. Öyleyse bu suç her iki seçimlik hareket yönünden de suçun işlenmesi ile sonlanması arasında bir süre bulunduğu için mütemadi suç özelliği gösteren fakat sisteme erişildiği/kalmaya devam edildiği anda suçun unsurları oluştuğu için ani suç özelliği de gösteren, ‘’muhtemel‘’ mütemadi suç[340] olarak nitelendirilmelidir.

Doktrinde genel kabul gören görüş, suçun sisteme erişme yönüyle icrai ve kalmaya devam etme yönüyle ise ihmali hareket ile işlenebilen bir suç olduğu görüşüdür.[341] Sisteme erişme hareketinin ihmali, kalmaya devam etme hareketinin ise icrai davranışlar ile gerçekleştirilip gerçekleştirilemeyeceği ise tartışmaya değer bir meseledir. Doktrinde Dülger, kalmaya devam etmenin icrai hareketler ile de gerçekleştirilebileceğini ve örneğin sistemle erişimi kesilmek istenilmesine ve bu yönde aktif bir çaba sarf edilmesine rağmen failin erişimin kesilmemesi için gerçekleştirdiği icrai davranışların bu şekilde değerlendirilmesi gerektiğini

[338] Ali PARLAR ve Mustafa ÖZTÜRK 2020, age. s. 28; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 239, 247; Hakan KARAKEHYA 2009, age. s. 13.
[339] İki ayrı suçun oluşmayacağı noktasında benzer yönde bkz. Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 902.
[340] Muhtemel mütemadi suçlara dair açıklamalar için bkz. Erdal YERDELEN (2014), ‘’Mütemadi (Kesintisiz) Suç‘’, *TAAD*, C. 5, S. 18, ss. 113-152 s. 117, 118.
[341] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 240; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 899, 900; Ali PARLAR ve Mustafa ÖZTÜRK 2020, age. s. 27, 28; Berrin AKBULUT 2017, age. s. 128; Muhammet Sefa ÇETİN 2021, age. s. 10.

belirtmektedir.[342] Gerçekten de gerek IPS gibi siber güvenlik uygulamalarının otomatik olarak yaptığı gerek BT çalışanlarının manuel olarak yaptığı ‘’erişimi kesme‘’ girişimlerine ve gerekse fiziki olarak kablonun porttan çıkartılmasına ya da bilgisayarın elinden alınmasına karşı aktif eylemlerde bulunan failin davranışı icrai olacaktır. Sisteme erişme yönünden de ihmali bir hareket neticesinde bu durumun doğması mümkündür. Örneğin botnet ağına dahil bir köle bilgisayar, kullanıcısı başında oturduğu sırada hackerın talimatları doğrultusunda üçüncü taraf sistemlere yetkisiz erişime yönelik işlemler gerçekleştirir ve kullanıcı bu durumun farkında olmasına rağmen tepkisiz kalır ise ihmal suretiyle gerçekleştirdiği fiili vasıtasıyla suça iştiraki ve asli failliği gündeme gelebilecektir.

3.2.1.4.1. Hangi Durumların Bilişim Sistemine Erişmek/Girmek Olarak Kabul Edileceği Sorunu

Donanım ve verilerin ayrılmaz bütünlüğünden meydana gelen bilişim sistemlerine erişmek, donanım boyutuyla bir cihazın kapağını söküp kart ve çiplere dokunmak değildir. Donanım ve verilerin birleşiminden oluşan bir yapıya erişmek, mecburen donanımlar vasıtasıyla var olan bir siber uzaya ulaşmak şeklinde tecelli edebilir.[343] Aynı şekilde ‘’omuz sörfü‘’ olarak nitelendirilebilecek olan, açık bir sistemin monitörünü sadece göz ile izlemek fiilleri de siber uzaya erişim olarak değerlendirilmeyecek, suça konu hareketin gerçekleştirilmesi için yetkisiz bir erişim durumunun siber uzay üzerinden yaratılması gerekecektir.[344] Zikredilen bu hususlar konusunda doktrinde bir tartışma yok ise de hangi neticelerin TCK md. 243 bağlamında, donanım ve verilerden oluşan bu yapıya ‘’erişmek‘’ olarak kabul edileceği konusunda ortak bir görüş yoktur.

Ağ bağlantısı yoluyla ya da fiziki bağlantılarla sistemdeki herhangi bir yazı, görüntü veya uygulama dosyalarına erişilebilir. Yine örneğin sistem çalıştırıldığı andan itibaren verilerin işlemesiyle canlanan işletim sistemi yazılımının ya da sistem içerisindeki sair yazılımların ve en basit şekliyle masaüstü ekranının ya da bu aşamaya gelinmeden sistemde çalışan BIOS ve sair ara birimlerdeki programların bilfiil

[342] Murat Volkan DÜLGER 2022, age. s. 269.
[343] Aynı yönde bkz. Ali PARLAR ve Muzaffer HATİPOĞLU 2010, age. s. 3743; Doğan SOYASLAN 2020b, age. s. 662; Hasan GERÇEKER 2020, age. s. 2153; Murat Volkan DÜLGER 2022, age. s. 267, 269, 270.
[344] Yavuz ERDOĞAN 2010, age. s. 1380; Ahmet Caner YENİDÜNYA 2005, age. s. 10; Dilek GÜLER 2018, age. s. 18.

çalıştırılması vasıtasıyla da sisteme erişilebilmektedir. Aynı şekilde kablolu ya da kablosuz ağ yapılarına ve örneğin bir wi-fi bağlantı noktasına bir şekilde yetkisiz olarak bağlanılarak ağa erişilebilmektedir. Doktrin ve yargı kararlarında da suça konu hareket/netice yönünden benzer örnekler verildiğinden,[345] bu gibi durumlarda neticeye yönelik bir tartışmanın söz konusu olmadığı açıktır. Örneklenen durumlarda doktrinde herhangi bir tartışmanın olmamasının sebebi, bu tür durumlarda nihayetinde ‘’algılanması basit yöntemlerle somut olarak erişilmiş‘’ bir sistemin bulunması ve failin hedef sistemdeki siber uzayı gözle ya da ekranı üzerinden görüyor yahut ağ ile bağlantı sağladığına dair bir geri bildirim alıyor olmasıdır.

Hacking yöntemlerinde kullanılan araçlar olan; hedef sisteme malware, komut, kod veya veri paketleri gönderilmesi sonucunda da sistemlerdeki verilere ulaşılabilmekte, bunlar kontrol edilebilmekte yahut sistemler üzerinde çeşitli işlemler gerçekleştirilebilmektedir. Lakin bu tür durumlarda, fail hedef sistemdeki siber uzayı fiilen gözle ya da kullandığı sistemin ekranı üzerinden görmemekte yahut duymamaktadır. Bir malware enjeksiyonunda, failin rootkitin oluşturduğu arka kapılar üzerinden sisteme bağlantı sağlaması ve keylogger işlevi gören diğer malware’in yaptığı kayıtlara erişmesi mümkündür. Bu durumda arka kapılar üzerinden hedef sisteme bilfiil bağlanılması, tartışmalı alanın dışında kalmaktadır. Ancak hackingde fail her zaman hedef sistem ile bu şekilde somut bir bağlantı kurmaz. Örneğin hedef sistemdeki açıkların veri paketleri gönderilerek taranması, aynı yöntemle hedef sisteme dair bilgilerin elde edilmesi, sisteme enjekte edilen malware’in sistemde kontrol yetkisine sahip olması ve ötesinde sistemdeki verilere dair bilgileri/verileri otomatik olarak faile göndermesi veya hedef sisteme zararlı kodlar enjekte edilerek benzer sonuçlara ulaşılması mümkündür. Tüm bu ayrık durumlar ise pratikte çok fazla tercih edilen eylem tipleri olmakla birlikte, hukuk perspektifinden alışılmış bir ‘’sisteme erişme‘’ vaziyetini yaratmamaktadır.

---

[345] TCK md. 243’e dair yargı kararlarının içeriği genellikle mail ya da sosyal medya hesaplarına veya ağ bağlantıları vasıtasıyla yetkisiz olarak erişilen sunucuların barındırdığı sair ortamlara dairdir. Mail hesabına yetkisiz erişime dair karar örnekleri için bkz. Yargıtay 8. CD 2015/2112 E. 2015/15394 K.; Yargıtay 8. CD 2013/10401 E. 2014/11835 K.; Yargıtay 8. CD 2018/10824 E. 2019/15723 K.; Yargıtay 12. CD 2015/9555 E. 2016/10731 K. / Sosyal medya hesabına/kullanıcı ara yüzüne yetkisiz erişime dair kararlar için bkz. Yargıtay 8. CD 2014/33371 E. 2015/15859 K. / Bankaların online platformları üzerinden banka hesabına yetkisiz erişime dair karar için bkz. Yargıtay 11.CD 2008/18190 E. 2009/3058 K. / Hard diske yetkisiz erişim örneği için bkz. Ali PARLAR ve Mustafa ÖZTÜRK 2020, age. s. 27 / İnternet ortamına yetkisiz erişim örneği için bkz. Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 901; Berrin AKBULUT 2017, age. s. 134.

Benzer bazı ‘’atipik‘’ durumların hacking haricinde de oluşması mümkündür. Örneğin bir USB’nin sadece bağlantı portuna takılması ya da modeme bağlantı kablosu ile bağlanılmasına rağmen yetkili MAC adresine sahip olunmadığı için ağa erişilmemesi ve bu yönde bir çaba da sarf edilmemesi gibi durumlar da ‘’sisteme erişme‘’ vaziyeti yönünden tartışılabilir. Başka ‘’atipik‘’ durumlar ise yetki ve aleniyet noktasından kaynaklanmaktadır. Örneğin bilgisayar ya da telefon gibi sistemlerin şifrelenmemiş olması durumunda hayatın olağan akışına göre bu durum sistemin alenen kullanımına izin verildiği anlamını taşımayacaktır. Bu sebeple hiç kimse masada duran bir telefonun şifresiz olduğunu anlayıp içeriğini karıştıramaz. Lakin aynı yorumun tarayıcıya URL girildiğinde ulaşılan deep web içeriklerinde doğrudan yapılması mümkün olmayabilir. Örneğin internet üzerinden erişilebilen ve sadece URL’yi bilen kişilerin ulaşabileceği bir intranet web sayfası bulunabilir. Bu web sayfaları ara yüz de olabilir ve eğer bu noktalarda şifreli erişim bulunmuyorsa, URL’yi öğrenen ve bağlanan kişinin gizlenmesi istenen verilere ulaşması hatta bunları değiştirmesi tehlikesi bulunacaktır.[346] Tarayıcıya URL girilmesi son derece masum bir durum gibi görünse de teoride bu durumun sadece şifreyi bilenlerin erişebileceği internet ortamlarından pek de farkı yoktur. Zira güvenlik açığı oluşturacak şekilde yaratılmamış ise bu tür URL’lere rastlantısal biçimde ulaşılması çok zordur.

Aşağıda evvela doktrinde yukarıdaki gibi ‘’atipik‘’ durumların bilişim sistemine erişmek yönünden ne şekilde anlaşıldığı açıklanmış ve bilahare de konuya dair şahsi değerlendirmelerde bulunulmuştur.

3.2.1.4.1.1. Atipik Eylemlerin Bilişim Sistemine Erişme Sayılıp Sayılmayacağına Dair Doktrin Görüşleri

Doktrindeki bazı görüşler, girme/erişme fiiline dair spesifik bazı örnek eylemler üzerinden çeşitli yorumlarda bulunmaktadır. Bu konuda öne çıkan en yaygın yorum, içtihatlarda da aynı ‘’mail-dosya‘’ örneği üzerinden yapıldığı üzere, sisteme veri/dosya gönderilmesinin sisteme erişmek sayılmayacağı yorumudur.[347] ASS Açıklayıcı Raporu’nda da ikinci maddedeki yetkisiz erişim suçuna yönelik, ‘’…

[346] Benzer örnekler için bkz. Bünyamin DEMİR 2020, age. s. 211, 212, 213 vd.
[347] Berrin AKBULUT 2017, age. s. 130, 131; Yargıtay, 8. CD 2017/7105 E. 13811 K. İçinde, Ahmet GÜL 2021, age. s. 98; ‘’*Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez.*‘’ Yargıtay 8. CD 2014/29566 E. 2015/13421 K.

Ancak, yalnızca bir e-posta mesajının veya dosyanın gönderilmesini içermez. ‘’ denilmektedir.

Bazı görüşler ise gönderilen yazılımlar aracılığıyla sisteme bağlanma ve verilere erişme imkanı doğuyorsa, yazılımın çalışması durumunda sisteme erişmeden bahsedilebileceğini, çalıştırılmaması ve veri olarak depolama biriminde yüklü kalmasında ise teşebbüsün gündeme gelebileceğini belirtmektedir.[348] ASS Komitesi/T-CY'nin botnetler hakkındaki rehber kılavuzunda da malware enjeksiyonu sonucu yapılan ‘’botnet ağı oluşturmanın‘’ yasadışı erişim kapsamında değerlendirilmesi gerektiği belirtilmiş ve sistemi kontrol edebilir olmak, sisteme erişmek şeklinde görülmüştür.[349]

Yukarıdaki görüşler, somut olarak hackerın malwareler üzerinden hedef sistemle bağlantı sağlaması ve bilfiil malware yazılımları kontrol etmesini şart koşmamıştır. Örneğin bir rootkit yazılım topluluğu sisteme enjekte olup çalışmaya başladığında, bu durumun ‘’sisteme erişim‘’ olarak kabul edilmesi için hackerın bağlanabileceği arka kapıların oluşturulması ve ağ bağlantısı kurularak veri alış-verişi yapılması, hedef sistemdeki dosyaların çekilmesi ya da malware'e komutlar gönderilmesi şart değildir. Zıt yöndeki bir görüşe göre ise sisteme erişim durumunun oluşabilmesi için hackerın malware gönderdiği sisteme, oluşturulan arka kapılar vasıtasıyla bilfiil erişerek bağlantı kurması gerekir.[350]

Doktrinde spesifik bir eylemi nitelemeden, bir sisteme TCK md. 243 bağlamında hangi durumda erişilmiş sayılması gerektiğine dair ‘’*sistemdeki verilere ulaşma ve müdahale imkanı doğduğu an*‘’ bu durumun gerçekleşeceği yönünde görüşler de mevcuttur.[351] Öyleyse yukarıda zikredilen atipik durumlar ve örneğin sisteme içeriden veri iletme, veri kaydetme, bozma, değiştirme, arka kapılar oluşturma ve sair yeteneklere sahip bir malware enjekte edilmesi ‘’erişme‘’ şeklinde

---

[348] Fatih Selami MAHMUTOĞLU (2013), *Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 71, S. 1i, 2013, ss. 855-889, s. 861; Hasan Burak ÖNDİN 2017, age. s. 35; Ahu Karakurt EREN (2020), ‘’Sızma testleri ile Türk Ceza Kanunu'nun 243, 244 ve 245/A Maddelerinde Düzenlenen Suçlar Arasındaki İlişkinin Değerlendirilmesi‘’, *Terazi Hukuk Dergisi,* C. 15, S. 164, ss. 747-764, s. 753 / Kanaatimizce bir malware yazılımın kurbanların indirmesi için internet ortamındaki bir dosyaya gömülmesi fakat kimsenin dosyayı indirmemesi durumunda da suç teşebbüs aşamasında kalacaktır. Bu durumun hazırlık hareketi olduğuna dair aksi yönde görüşler için bkz. Ahmet GÜL 2021, age. s. 112.

[349] T-CY (2013), *Guidance Note 2, Provisions of The Budapest Convention, Covering Botnets*, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168002e7094, (ET: 02.03.2022).

[350] Şaban Cankat TAŞKIN 2008, age. s. 29.

[351] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 238.

değerlendirilebilecektir. Aynı imkanları doğuran bir kodun enjekte edilmesi ya da veri paketi gönderilmesi durumları da bu kapsamda kalabilecektir. Buradaki sorun şudur, her malware hedef sistemde çeşitli işlemler gerçekleştirebilmek veya hedef sisteme dair çeşitli verileri elde edebilmek amacını taşır. Örneğin salt virüs özelliği gösteren ve verilerin öğrenilmesine değil zarar verme amacına yönelen bir malware de hackera otomatik de olsa bir ‘’sisteme müdahale‘’ imkanı sağlamaktadır. Bu sebeple ancak sistem içerisinde herhangi bir işlem yapamayan yani düzgün çalışmayan bir malware'in enjekte edilmesi durumunda ‘’*sistemdeki verilere ulaşma ve müdahale imkanı*‘’ doğmayacak ve sisteme erişme durumu söz konusu olmayacaktır. Eğer ilgili görüşte ‘’ve‘’ bağlacı verilere ulaşma + müdahaleye dair her iki yetkinliğin birlikte olması gerektiği yönünde ise şüphesiz ki bu iki yetkinliği kazandıramayan sair malware enjeksiyonları da gündeme gelebilir. Doktrindeki sair bir görüş bu yönde olup, bir malware sistemdeki veriler üzerinde hakimiyet kuruyor fakat failin sistem içerisindeki verileri görmesine imkan sağlamıyorsa sisteme erişme durumunun oluşmayacağını belirtmektedir.[352]

3.2.1.4.1.2. Değerlendirme

Hangi spesifik eylemler sonucunda bir bilişim sistemine ‘’erişilmiş‘’ olunacağı noktasında eylem tipleri tek tek incelenemeyeceğine göre burada bir çerçeve eylem modeli belirlemek şarttır. Bu noktadaki en doğru yorum, yukarıda zikredilen ‘’s*istemdeki verilere ulaşma ve müdahale imkanı doğduğu an*‘’ bu durumun gerçekleşeceği yönündeki görüştür.[353] Lakin kanımızca ‘’*sistemdeki verilere ulaşma ve/veya sistem içeriğine kontrol altında bir müdahale imkanı doğduğu an*‘’ sisteme erişilmiş kabul edilmeli ve her iki yetkinlik durumunun bir arada gerçekleşmiş olması şart koşulmamalıdır. Sistem içeriği yani siber uzaya dair müdahale imkanının da ‘’kontrol altında‘’ bir müdahaleye dair olması gerekir. Örneğin sistemdeki verilere rastgele zarar veren ve başka hiçbir yetkinliği hackera sağlamayan bir virüsün mağdur tarafından indirilip çalıştırılmasının, hackerın faili olduğu bir ‘’sisteme erişme‘’ neticesi şeklinde yorumlanması mümkün değildir. Zira bu neticeyi virüsü internet ortamına salan kişiler öngörmüş olsalar bile mağdura yönelik kontrolleri altında yahut planladıkları bir netice gerçekleşmemekte, ‘’erişme‘’ şeklinde algılanabilecek bilinçli bir müdahale de olmamaktadır. Öyleyse salt hedef sistemde önceden planlanmış

[352] Emre İkbal AÇIKGÖZ 2017, age. s. 98.
[353] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 238.

işlemleri gerçekleştiren veya ileride kendisine gönderilecek komutları uygulayacak yani ‘’kontrol altında işlemler gerçekleştirecek‘’ malware yazılımların enjeksiyonu, sisteme erişme şeklinde yorumlanmalıdır.

Sistemdeki verilere ulaşma ve/veya sistem içeriğine kontrol altında bir müdahale imkanı doğduğu an sisteme erişilmiş kabul edileceğinden; bir swithcin fiziki portuna kablolu bağlantı sağlamak fakat kablonun diğer ucundaki bilgisayar üzerinden ağa katılmamak, bir bilgisayarın usb portuna usb belleği yalnızca takmak ve benzeri durumlarda bu imkanlar doğmadığından, bu eylemler sonucu hedef sisteme erişilmiş sayılamaz. Aynı şekilde IP sorgusu, işletim sistemine ya da açık portlara dair bilgilere ulaşmaya veya hedef sistemdeki sair bilgilerin taranmasına yönelik sorgu istekleri yollanması/veri paketleri gönderilmesi durumlarında da hedef sistemden dönen otomatik cevaplardan ‘’*sistemdeki verilere ulaşma ve/veya sistem içeriğine kontrol altında bir müdahale imkanı*‘’ doğmayacağından, bu durumlar da hedef sisteme erişim sayılamaz.

3.2.1.4.1.2.1. Malware Enjeksiyonu ve Sisteme Erişim İlişkisi

Yalnızca hedef sistemde önceden planlanmış işlemleri gerçekleştiren veya ileride kendisine gönderilecek komutları uygulayacak olan yani ‘’kontrol altında işlemler gerçekleştirecek‘’ malware yazılımların enjeksiyonunun sisteme erişme şeklinde yorumlanabileceği yukarıda zikredilmişti. Bir bilişim sistemine malware enjekte edilmesi yönünden bu noktada tartışılması gereken mesele, bilişim sistemine ‘’erişmeden‘’ yapılan enjeksiyonlar yönündendir. Zira sisteme eriştikten sonra failin direkt olarak malware enjekte etmesi durumunda, yetkisiz erişim suçu yönünden tartışılacak bir husus bulunmamaktadır.

Hedef sisteme erişmeden verilerin gönderilmesi ve bu veri dosyalarının hedef sisteme kaydedilmesi iki şekilde gerçekleşebilir. Bunlardan ilki, işlemi bir aracının yapması ve örneğin mailin alıcı tarafının uygulama yazılımından mail sunuculara erişerek, mail içerisindeki dosyaları kendi sistemine bizzat kaydetmesidir. Bu gibi durumlarda malware’in hedef sisteme fail tarafından doğrudan enjeksiyonu değil, mağdurun kendi sistemine bu verileri yerleştirdiği durumlar meydana gelir. Benzer örnekler; mağdura içerisinde malware barındıran bir CD verilmesi ve mağdurun bunu bilgisayarında çalıştırması, çeşitli bağlantılar içine indirme linkleri gizlenerek mağdur tıkladığında malware’in indirilmesinin amaçlanması veya bu yönde sair yöntemlerdir. Hedef sisteme erişmeden verilerin gönderilmesi ve bu veri dosyalarının hedef sisteme

kaydedilmesinin ikinci şekli ise verilerin bir aracı olmadan, doğrudan hedef sistemde kaydedildiği durumlardır. Böyle bir durumda mağdurun malware'i bizzat yüklemesi değil, hackerın doğrudan enjekte etmesi durumu gerçekleşir. Örneğin Whatsapp'ta her ne kadar Whatsapp sunucuları da bu verileri bir süre saklıyor ise de ilgili özellik açılmışsa, bir dosya gönderiminde direkt olarak telefonun hafıza birimine bu dosya kaydedilir.

Hedef sistemi ele geçirmeden ve sisteme erişmeksizin, sistemin salt okunur belleği ya da depolama ünitelerinde alan işgal edecek veri dosyaları enjekte etmek/kaydetmek yönünden aşılması gereken temel mesele, bu durumun TCK md. 244/2 ile bağlantısıdır. Belirtmek gerekir ki hedef sistemi kontrol altına almadan veya hedef sisteme erişim sağlamadan gönderilen verilerin hedef sisteme direkt olarak kaydedilebilmesi, yalnızca bu durumun teknolojinin işleyişinden kaynaklandığı zaman mümkündür. Eğer hedef sistemler belirli kanallardan gelen veri trafiğini direkt olarak kaydedecek şekilde programlanmışsa, birine mail gönderildiğinde mail servisini işleten İSS'nin sunucularına bu mailin otomatik kaydında olduğu gibi ''veri kaydı yönünden'' herhangi bir hukuksuzluk gündeme gelmeyecektir. Bu sebeple sisteme erişmeden gönderilebilecek veriler noktasında TCK md. 244/2 bağlamında bir değerlendirme yapılmasına gerek yoktur. Lakin malware enjeksiyonunda mağdur veya sair bir üçüncü kişinin aracı kılınması durumunda, TCK md. 244/2'nin de oluşabileceği[354] ve bu durumun içtima noktasında değerlendirilmesi gerektiği belirtilmelidir.

Öyleyse nihai olarak denilebilir ki eğer hedef sistem ele geçirilmeden/sisteme erişilmeden bir malware hedef sisteme yukarıdaki ihtimaller dahilinde bir şekilde enjekte edilmiş ise ve bu malware ''*sistemdeki verilere ulaşma ve/veya sistem içeriğine kontrol altında bir müdahale imkanını*'' sunabilecek özellikteyse, yazılımın otomatik olarak veya mağdurun müdahalesi sonucu çalışması sonucunda sisteme erişilmiş olduğu kabul edilmelidir. Bu yüzden TCK md. 243 bağlamında hackerın daima hedef sisteme bilfiil bağlanması şart değildir. Yazılımın çalıştırılmaması veya düzgün çalışmayarak bu imkanları sağlamaması durumunda ise doktrinde de belirtildiği üzere suçun teşebbüs halinde kaldığından söz edilecektir.[355]

[354] Bu gibi durumlarda hackerın TCK md. 244/2 yönünden dolaylı fail olarak değerlendirilmesi gerektiği yönünde görüşler için bkz. Olgun DEĞİRMENCİ 2019, age. s. 193, 194.
[355] Fatih Selami MAHMUTOĞLU 2013, age. s. 861; Ahu Karakurt EREN (2020), age. s. 753.

3.2.1.4.1.2.2. Kod, Komut veya Veri Paketi Gönderimi ve Sisteme Erişim İlişkisi

Hacking yöntemleri aktarılırken detaylandırıldığı üzere, bir sistemde çalıştırılan programlama dillerini manipüle edecek sorgular ve veri paketleri gönderilerek, sistemdeki verilere ulaşılabilir. Örneğin istemciden gelen verileri düzgün filtrelemeden sunucu tarafında çalıştıran bir veri tabanı oluşumunda, arka yüzde SQL dili kullanılıyorsa bu dili manipüle edecek ve yetkisiz olarak erişilememesi gereken noktalara hackerı eriştirecek SQL komutları hedef sisteme gönderilebilir. SQL enjeksiyonu sonrasında yetkisiz olarak hedef sunuculardaki veri tabanına erişilebileceği gibi bu veri tabanı üzerinde çeşitli işlemler de gerçekleştirilebilmektedir. Kırılmış erişim kontrolü yöntemiyle de URL adreslerine hedef sistemde çalışan yazılımları manipüle edecek girdiler girilebilir ve hedef sunucuda bu yönde bir güvenlik açığı varsa, üçüncü taraf kullanıcıların bilgilerine/sisteme yetkisiz olarak erişilebilir. Öyleyse ‘’*sistemdeki verilere ulaşma ve/veya sistem içeriğine kontrol altında bir müdahale imkanı*‘’ sağlamanın ötesinde direkt olarak sisteme erişimi gerçekleştiren bu durumların, sisteme erişme olarak değerlendirilmesi gerekmektedir.

Kod enjeksiyon saldırılarında, kodları değiştirilen ve bu sebeple sunucu tarafındaki yazılımların çalışması bozulan web sitesi vasıtasıyla, siteyi ziyaret edenlerin cookie ve sair bilgileri elde edilerek yahut sair şekillerde kullanıcı ara yüzlerine direkt olarak erişilebilmektedir. Bu noktada da ‘’*sistemdeki verilere ulaşma ve/veya sistem içeriğine kontrol altında bir müdahale imkanı*‘’ sağlamanın ötesinde direkt olarak sisteme erişim gerçekleştiğinden, bu durumların da sisteme erişme olarak değerlendirilmesi gerekmektedir. Lakin bir XSS saldırısında hedef sisteme enjekte edilen ve örneğin bir web sitesinin kaynak kodları arasına yerleştirilen zararlı kodların kullanımı ya da doğrudan bir banner’a veya internetteki bir resme tıklandığında hedef sistemde otomatik olarak bazı komutları çalıştıracak kodların enjeksiyonu durumlarında, genellikle hedef sistemlerde bir hakimiyet elde edilmez ya da veriler görünür hale gelmez. Örneğin kodları arasına bir satır olarak zararlı Java kodunun enjekte edildiği web sitesine bağlanan bir istemci sistem, kodun tetiklediği komutların çalıştırılmasıyla kullanıcısının onayı olmaksızın otomatik olarak bir kısım işlemler gerçekleştirir. Bu tür durumlar ise kanaatimizce yalnızca TCK md. 244/2’nin tipikliği içerisinde değerlendirilmelidir.

3.2.1.4.2. Bilişim Sisteminin Bir Kısmına ve Sanallaştırılmış Birimlere Erişim Durumları

TCK md. 243/1'in lafzında ''*Bir bilişim sisteminin bütününe veya bir kısmına ...*'' denilerek, seçimlik hareketlerin bilişim sisteminin bütününe yönelik gerçekleştirilebileceği gibi bir izlenim oluşturulmuştur. Lakin nasıl ki konut dokunulmazlığını ihlal suçunun oluşabilmesi noktasında evin tüm odalarına tek tek girilmesi yönünden bir özellik bulunmuyor, yaralama suçunda bütün uzuvlara darbe vurulup vurulmadığı önemsenmiyor ya da mala zarar verme suçunda malın ''tamamına veya bir kısmına zarar verilmesi'' gibi bir ayrım yapılmıyor ise bilişim sistemine yetkisiz erişim suçu yönünden de normun lafzında böyle bir ayrımın yapılmaması gerekirdi. Hatta bu tür bir ayrımın bilişim sistemleri ile ilişkili normlarda hiç yapılmaması gerekir. Zira donanım ve verilerin ayrılmaz bütünlüğünden meydana gelen bilişim sistemlerinin erişilebilecek somut bir ''bütünü'' yoktur. Örneğin mobil sistemlerin hafıza kartları, dahili gömülü depolama üniteleri ve sim kartlarında çeşitli veriler barındırılmaktadır ve cep telefonuna yetkisiz erişen kişi sadece dahili hafızada barındırılan uygulama yazılımlarını çalıştırmış olabilir.[356] Böyle bir durumda mobil sistemin tamamına erişim hakimiyeti sağlamış kişinin, sistemin ''veri boyutuyla'' bir kısmına eriştiği doğru olsa bile bu olgunun suça etki edebilecek bir özellik göstermesi mümkün olamaz. Zira fail telefondaki her noktaya erişmeye çalışsa bile bir kısım sistem dosyasına ulaşamayabileceğinden, sistemin ''bütününe'' erişmesi fail istese de zaten mümkün olamayabilir. Öyleyse tek bir sistem içindeki herhangi bir kısma erişmek bizatihi bilişim sistemine erişmek olarak kabul edilmeli ve ''tek sistemin bütününe erişmek/bir kısmına erişmek'' noktasında suçun işlenme biçimi bakımından bir ayrım yapılmamalıdır. Zira aksi bir yorumda bilişim sistemi üzerinde gerçekleştirilen her işlemde sistemin farklı bir kısmına erişilmiş olacağından, sürekli işlem sayısınca farklı suçların oluşması ve erişim kesilene kadar paradoks gibi sonsuz sayıda bilişim sisteminin bir kısmına erişim suçunun işlenmesi söz konusu olacak, bu durum aynı zamanda bir zincirleme suç karinesi de doğuracaktır. Şüphesiz ki bu kabul edilemez bir yorum olup, normun ruhuna da apaçık biçimde aykırıdır.

Bilişim sistemlerinin içeriğindeki siber uzaya dair ''farklı kısımlar'' noktasında dikkate alınması gereken esas durum, tek bir fiziki bütünlük içerisinde iki

[356] Bu konuda detaylı bilgi için bkz. Ahmet EKİM (2013), *Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi ve Raporlanması*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Gazetecilik Ana Bilim Dalı Yüksek Lisans Tezi, İstanbul, s. 56, 57 vd.

ayrı sistemin bulunup bulunmadığı hususudur. Yani tek bir fiziki bütünlük arz eden cihazda; ‘’*tek bilişim sistemi içerisindeki farklı kısımlar*‘’ mı bulunmaktadır, yoksa ‘’*birden fazla bilişim sistemi ve bu sistemler içerisindeki farklı kısımlar*‘’ mı bulunmaktadır sorusu cevaplandırılmalıdır.

Ağ yapılarının, sunucuların, sistemlerdeki dahili depolama birimlerinin, işletim sistemlerinin ve sistemlerdeki siber uzaya dair sair unsurların sanallaştırılarak, soyut sınırlar ile birbirlerinden ayrıldığı sanallaştırma uygulamaları işte tam da bu noktada önem arz etmektedir. Tezin ikinci bölümünde zikredildiği üzere sanallaştırılmış bölümler donanım boyutuyla bir sistem içerisindeki farklı veri alanlarını doldurduklarından, nihayetinde tek bir fiziksel bütünlüğü olan sistemin bir bölümündeki ayrık bilişim sistemleri olarak kabul edilmelidir. Fiziki yahut sanal tek bir sistem içerisindeki farklı veriler ise tek bir sistem içerisindeki ‘’sistemin farklı kısımları‘’ olarak değerlendirilebilir. Bu durum tıpkı bir apartmandaki farklı dairelerin ayrı ayrı taşınmazlar olarak kabul edilmesine fakat ev arkadaşlarının odalarının tek bir taşınmaz içerisinde değerlendiriliyor olmasına benzer. Öyleyse tek bir sistem üzerindeki on ayrı sanal birimden her birine yapılan ayrı yetkisiz erişimler farklı suçlar doğurmalıdır. Lakin içeriği sanallaştırılmamış sistemlere veya sanal birimlerin içeriğindeki farklı farklı depolama alanlarına ve/veya farklı yazılımlara (*yani farklı kısımlara*) erişilmesi, tek bir sisteme erişim suçunun icrasına konu faaliyetler kapsamında değerlendirilmelidir.

Örneğin iki kişinin ortak kullanımında olan bir sistemde tek bir kullanıcı oturumu içerisindeki dahili depolama biriminde ayrı kişilerin kullanımına tahsis edilmiş iki ayrı klasör bulunabilir ve bu klasörlerin her ikisinin de farklı şifreleri olabilir. Fail her klasöre de erişir ise burada tek bir sistem içerisindeki farklı kısımlara erişim söz konusu olduğundan iki ayrı suç oluşmamalı, hisseli tapulu bir taşınmaza karşı işlenen suçlarda olduğu gibi tek suçun iki mağdura karşı işlendiği kabul edilmelidir. Lakin eğer sistemde iki ayrı kullanıcı ara yüzü/oturumu/sanal birim/yetki ayrımı bulunuyor ve/veya işletim sistemi sanal birimlere ayrılıyor ise bu durumda sistemin bütünü tek bir kişiye ait olsa bile her iki sanal birime ayrı ayrı erişilmesi, tek mağdura karşı işlenmiş iki ayrı suç olarak kabul edilmelidir.[357]

[357] Farklı suçların oluşacağına dair benzer görüşler için bkz. Muammer KETİZMEN 2006, age. 125, 126 vd. / Sanal birimlere dair benzer lakin tek birim içerisindeki farklı veri alanlarının farklı kullanıcılara ait olması durumunda da farklı suçların oluşacağı belirtildiğinden bu noktada zıt yönde görüşler için bkz. Ramazan DOĞAN 2014, age. s. 60, 61.

3.2.1.4.3. Bilişim Sisteminde Yetkisiz Olarak Kalmaya Devam Etmek Durumunun Oluşabileceği Haller

Suça konu bir diğer seçimlik hareket, bilişim sisteminde yetkisiz olarak kalmaya devam etmektir. Bilişim sistemine erişme durumunun aksine bir kişinin sistemde kalmayı hangi eylemleriyle gerçekleştirebileceği tartışmalı bir husus olmayıp, anlık sisteme erişim sonrası bu mevcut durum devam ettirildiği her an sistemde kalınmış olacaktır.[358] Sistemde kalmaya devam etme yönünden tartışılması gereken esas mesele, bunun yetkisiz olarak nasıl yapılabileceği ve yetkili olarak erişilen bir sistemde yetkisiz şekilde kalmaya devam etme yönünden bir asgari sürenin söz konusu olup olmadığıdır.

Doktrinde, suçun yalnızca ‘’bir sistemde yetkisiz olarak kalmaya devam etme‘’ seçimlik hareketi sonucu oluşabilmesi için hukuka uygun/yetkili olarak erişilen sistemde erişim sürerken, rızanın geri alınması gibi bir durumun oluşması ve sistemde kalmanın o andan sonra yetkisiz hale gelmesi gerektiği belirtilmektedir.[359] Gerçekten de eğer failin sisteme erişimi bizzat yetkisiz ise bu durumda suç direkt olarak ‘’sisteme yetkisiz erişim‘’ seçimlik hareketi sonucunda doğacak, sisteme yetkisiz olarak kalmaya devam edilmesi de yetkisiz erişim fiilinin işlenmeye devam etmesi olarak algılanacaktır. Eğer fail sisteme yetkisiz olarak erişir ve erişimi devam ederken mağdur ile anlaşarak geleceğe yönelik ve örneğin otuz dakikalık bir rızasını alırsa, süre bittikten sonra sisteme erişimini kesmemesi durumunda hem sisteme yetkisiz erişim hem de sistemde yetkisiz olarak kalmaya devam etme seçimlik hareketleri yönünden bu suçun ayrı ayrı oluşması mümkün olacaktır.

Beşeri olaylarda bazen insanlar ağır hareket edebilir, geç algılayabilir veya anlık duraksamalar yaşayabilirler. Bu sebeple yetkisiz olarak sistemde kalmaya devam etme durumunda, süre meselesinin her durumda kendi özelinde tartışılmasında fayda olabilir. Buradaki sorun, sürenin suçun hangi unsuru yönünden dikkate alınacağıdır. Doktrindeki katıldığımız görüşler, sürenin suçun objektif tipikliği yönünden bir öneminin olmadığı ve bu durumun cezanın bireyselleştirilmesi noktasında hüküm kurulurken ele alınması gereken bir mesele olduğu yönündedir.[360] Bir kısım

[358] Hasan GERÇEKER 2020, age. s. 2153.
[359] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 239; İbrahim ŞAHBAZ 2020, age. s. 3124; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 902; Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 961; Meral EKİCİ ŞAHİN ve Irmak KORUCULU 2019, age. s. 598.
[360] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 961; Berrin AKBULUT 2017, age. s. 136.

görüş ise evvela sisteme erişim durumunun oluşabilmesi için belirli bir süre sistemde kalınması gerektiğini, anlık girip çıkmaların bu sonucu oluşturmayacağını dile getirmektedir.[361] Objektif tipiklik bakımından sürenin, her durumun kendi özelinde ayrıca dikkate alınması gerektiği yönünde görüşler de mevcuttur.[362] Başka bir görüş ise kalmaya devam etme seçimlik hareketi vasıtasıyla bu suçun oluşabilmesi için cezalandırmaya yeterli, korunan değerleri ihlal edecek seviyede bir sürenin bulunması gerektiğini belirtmektedir.[363]

Sürelerin suçun unsurları yönünden bir önemi bulunsa da bu önem objektif tipikliğin konusu değildir. Yukarıda da belirtildiği üzere, kanaatimizce suç her iki seçimlik hareket yönünden de ani suç özelliği de gösteren bir muhtemel mütemadi suçtur. Zira sisteme ya erişilmiş ya da erişilmemiş, sistemde ya kalınmış ya da kalınmamıştır. Bu durumun bir milisaniyelik bir zamanda ya da aylar boyunca gerçekleşmiş olması objektif tipikliğin değil, sübjektif tipikliğin ya da suçun hukuka aykırılık unsurunun konusu olabilir ve nihayetinde verilecek cezaya dair değerlendirmelerin bir kriterini teşkil edebilir. Öyleyse hukuka uygun biçimde sistemde erişim sürerken; yetkiye dair sürenin dolması, rızanın geri alınması veya sair şekillerde meydana gelen ‘’*hukuka aykırı olarak sistemde kalmaya devam etme*‘’ durumunda, suça konu hareket/neticenin gerçekleşebilmesi için belirli bir süre aranmayacaktır.

3.2.1.5. İlliyet Bağı

Objektif sorumluluk sistemine dayalı sorumluluk teorilerinde ve pekala sübjektif sorumluluk sistemini benimseyen Türk ceza hukukunda illiyet bağı, objektif tipikliğin zaruri bir unsurudur. Hareket ve hareketten dolayı meydana gelen netice arasındaki bağlantıya ve neticenin hareketin bir sonucu oluşuna illiyet bağı denilmektedir. Nedensellik bağı bugün için Türk hukukunda çoğunlukla uygun sebep teorisi, şart teorisi + objektif isnat edilebilirlik ve karma nedensellik teorisi olarak üç farklı teori çerçevesinde değerlendirilmektedir.

Bilişim sistemine yetkisiz erişim suçu, neticesi harekete bitişik bir suçtur. Normun üçüncü fıkrasındaki neticesi sebebiyle ağırlaşmış hal yönünden ise netice hareketten bağımsız olarak oluşmaktadır. Neticesi harekete bitişik suçlarda illiyet

[361] Cengiz APAYDIN 2017, age. s. 2153.
[362] Murat Volkan DÜLGER 2022, age. s. 272, 273.
[363] İbrahim ŞAHBAZ 2020, age. s. 3127; Hasan Burak ÖNDİN 2017, age. s. 35.

bağına dair bir değerlendirme yapmamak, dolaylı olarak illiyet bağı karinesine neden olacaktır. Öyleyse illiyet bağına dair tartışmalar, suçun unsurları yönünden es geçilmemesi gereken hususlar durumundadır. Zira bu tür suçlarda da pekala üçüncü kişilerin fiili, sistemin işleyişi ve sair sebepler, harekete bitişik durum/neticenin oluşumunu etkilemektedir. Kanaatimizce yetkisiz erişim suçu yönünden illiyet bağının ve bu yönde benimsenecek teorilerin tartışılması da özel bir önem arz etmektedir. Öyle ki bilişim sistemine yetkisiz erişim ve yetkisiz olarak sistemde kalmaya devam etme durumları, teknolojinin işleyişiyle doğrudan bağlantılıdır. Teknoloji ise hata payı içerir, bozulabilir veya hacker gibi üçüncü tarafların müdahalesi devreye girebilir.

Somut örnekler vermek gerekirse; mitm pozisyonundaki bir sunucu üzerinden X noktasına erişmesi gereken internet kullanıcısı, sunucunun ayarlarını değiştiren bir hacker sebebiyle Y noktasına ulaştırılabilir. Bu durum bir DDoS etkisi yaratacak şekilde çok fazla internet kullanıcısı daha aynı Y noktasına çıkartılabilir. Eğer Y noktası maksimum elli kişinin internet üzerinden aynı anda trafiğe dahil olacağı düşünülerek tasarlanmış bir intranet ortamı ise bu aşırı yük sayesinde sistem düzgün çalışmayacaktır. Sunucunun hata vermesi ihtimaline ek olarak bu gibi durumlarda düzgün çalışmayan sistemin istemcileri şifresiz olarak içeriğe ulaştırması da mümkün olabilir. Bu şekilde de internet kullanıcıları, üçüncü tarafın müdahalesi sonucunda yetkisiz olarak bir bilişim sistemine erişebilir. Yine zararlı kodlar gömülmüş bir mail açıldığı an sistemde çalıştırılan komutlar dolayısıyla sistem, üçüncü taraf bir sunucuya SQL enjeksiyon atağı gerçekleştirebilir ve bu sunucunun içeriğine yetkisiz olarak erişebilir. Aynı şekilde mail içerisindeki dosyaya tıklandığı anda sisteme malware yüklenebilir, zararlı kodların çalıştırdığı komutlar dolayısıyla sistem otomatik olarak kayıtlı tüm maillere bu malware'i gönderebilir. Bu tür durumlarda illiyet bağı üçüncü kişi hackerın müdahaleleri gereğince kesildiğinden, sübjektif tipikliğin değerlendirilmesine gerek olmadan suçun oluşmadığı sonucuna varılabilecektir.

Uygun sebep teorilerinde hareketin neticeyi gerçekleştirme uygunluğu,[364] objektif isnadiyet teorisinde ise şart teorisine göre kurulan illiyet bağının tehlikelilik, risk ve sair kriterlere göre objektif olarak faile isnat edilip edilemeyeceği tartışılır.[365]

---

[364] Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 204, 205.

[365] Veli Özer ÖZBEK (2010), *TCK İzmir Şerhi Türk Ceza Kanunu'nun Anlamı Cilt 1*, Seçkin, Ankara, s. 317, 318, 319, 320, 321, 322 vd.; Bernd HEİNRİCH (2014), *Ceza Hukuku Genel Kısım 1*, Ed. Yener Ünver, Çev: Hakan Hakeri, Yener Ünver vd., Adalet, Ankara, s. 127, 148; Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 188, 189, 190, 191 vd.; İzzet ÖZGENÇ (2005), *Türk Ceza Kanunu Gazi Şerhi(Genel Hükümler),* Seçkin, Ankara, s. 212, 213, 214, 215 vd.; Berrin AKBULUT 2018, age. s. 312;

Bilişim sistemlerinin teknolojisinden kaynaklı hatalarda, salt bu hatadan kaynaklı makine davranışları sonucunda bir sisteme yetkisiz olarak erişilir ise bu durumda sübjektif tipikliğin değerlendirilmesine gerek olmayacaktır. Zira bu tür neticeler uygun sebep teorisine göre atipik olacağından illiyet bağını kesecek, objektif isnadiyet teorisine göre ise teknolojik gelişmelerden kaynaklı izin verilen risk çerçevesinde kalacağı için netice faile isnat edilemeyecektir. Eğer sistem üçüncü kişi tarafından bilerek bozulmuş ise bu durumda da üçüncü kişinin fiili illiyet bağını kesecek, duruma göre bu üçüncü kişi dolaylı fail konumuna gelebilecektir.

Belirtmek gerekir ki istisnai durumları bilenlerin/hesaplayabilenlerin, usta hackerların ve bilişim uzmanlarının varlığı sebebiyle karma nedensellik teorisinin değerlendirilmesi doğru olacaktır. Zira gerek uygun sebep gerekse objektif isnadiyet teorileri, belirli objektif kıstaslar dahilinde değerlendirmeler yapar. Ancak beşeri düzende çizginin dışında yaşanan olaylar da bulunmaktadır ve gerçekten de eğer bir fail sistemdeki hatayı ve bu hatanın bir bilişim sistemine yetkisiz erişim/kalmaya devam etme neticesini doğuracağını hesaplayabiliyor ise ilgili teoriler failin beraat etmesine sebep olacaktır.

Karma nedensellik teorisinde ise illiyet bağı evvela objektif kıstaslara ve daha sonra da fail yönünden sübjektif kıstaslara göre değerlendirilir. Bu sebeple bilişim sisteminde olmaması gereken bir hata sonucu çok istisnai bir durum gelişir ve sistem hatalı biçimde üçüncü bir sisteme yetkisiz olarak erişirse, bu durum objektif olarak öngörülemez sayılacaktır. Fakat eğer fail bu durumu sübjektif olarak öngörebilmiş veya hatayı biliyor ise karma nedenselliğe göre illiyet bağı var sayılacak ve objektif tipikliğin oluşmaması nedeniyle beraat kararı verilmeyecektir.[366]

3.2.2. Sübjektif Tipiklik

3.2.2.1. Kast ve Haksızlık Bilincinin Bulunması Gereği

Faillerin iradi fiillerinin neticelerini öngöremiyor olsalar bile illiyet bağının varlığı durumunda neticeden sorumlu tutuldukları sistemler, objektif sorumluluğa dayalı ceza hukuku sistemleridir.[367] Sübjektif sorumluluk ise kast ve taksire bağlı

Timur DEMİRBAŞ (2021), *Ceza Hukuku Genel Hükümler*, Seçkin, Ankara, s. 271, 272; Bahri ÖZTÜRK ve Mustafa Ruhan ERDEM 2021, age. s. 231, 232, 233 vd.

[366] Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 225, 226, 227, 228; İzzet ÖZGENÇ 2021, age. s. 193, 194; Doğan SOYASLAN 2020a, age. s. 354, 355.

[367] Nazmiye ÖZENBAŞ (2012), *Neticesi Sebebiyle Ağırlaşmış Suçlarda Ceza Sorumluluğunun Esası,* Adalet, Ankara, s. 28, 29, 52; Koray DOĞAN (2015), *Neticesi Sebebiyle Ağırlaşmış Suçlar*, Adalet, Ankara, s. 91.

olduğundan, failin neticeye sebep olan hareketini gerçekleştirirken sahip olduğu bilinci temel alan bir sistemdir. Failin neticeyi kast veya taksir derecesinde bir bilinçle gerçekleştirebilmesi için evvela neticenin fail açısından sübjektif olarak öngörülebilir olması gerekir. TCK md. 22'ye göre taksirle bir neticeye sebep olan fail ancak kanun maddesinde bu tür bir sorumluluk düzenlemesi mevcut ise neticeden sorumlu tutulabileceğinden ve TCK md. 243'te de taksire dair bir düzenleme bulunmadığından, suçun taksir derecesinde bir bilinç ile işlenmesi mümkün değildir. TCK md. 21'e göre suçun oluşması kastın varlığına bağlı olduğundan, yetkisiz erişim suçu ancak kasten işlenebilen bir suç olmaktadır.

TCK md. 21'e göre kast, suçun kanuni tanımındaki unsurların bilinmesi ve istenmesi sonucunda meydana gelir. Öyleyse sübjektif tipikliğin oluşumu için neticenin öngörülebilir olması veya öngörülmesi yetmeyecektir. Bunun için failin evvela eylemleri vasıtasıyla eriştiği yapının bir bilişim sistemi olduğunu bilmesi ve ayrıca bilişim sistemine yönelik gerçekleştirdiği eylemlerin bu sisteme yetkisiz olarak erişmek veya sistemde yetkisiz olarak kalmak durumuna sebep olacağını istemesi şarttır.

Doktrindeki genel eğilim, bu suçun doğrudan/genel kastla işlenebileceği ve failin belirli bir saik ile hareket etmesinin yani özel kastın gerekmediğidir.[368] Doğrudan kasta ek olarak, normun lafzında ''*hukuka aykırı olarak*'' denildiği ve kast da TCK md. 21'e göre suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesi olduğundan, failde haksızlık bilincinin de bulunması gerekir.[369] Bu sebeple sisteme ''haksız olarak'' eriştiği veya kalmaya devam ettiği bilincine sahip olmayan fail yönünden TCK md. 243 nazarında tipikliğin sübjektif unsuru oluşmayacaktır.[370]

---

[368] Ali KARAGÜLMEZ 2014, age. s. 208; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 243; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1155; Ali PARLAR ve Mustafa ÖZTÜRK 2020, age. s. 27.

[369] Doğan SOYASLAN 2020b, age. s. 664; Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2012, age. s. 444; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 903; Berrin AKBULUT 2017, age. s. 139; Tunç DEMİRCAN 2007, age. s. 93; Meral EKİCİ ŞAHİN ve Irmak KORUCULU 2019, age. s. 607; Cengiz APAYDIN 2017, age. s. 72, 75; İsmail ERGÜN (2008), *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Adalet, Ankara,s. 90; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 243, 244 / Bazı görüşler TCK md. 243 yönünden hukuka aykırılık bilincinin gerekli olduğunu belirtmekte ise de bunu suçun hukuka aykırılık unsuru içinde incelemektedirler. Bu konuda bkz. Ahmet Caner YENİDÜNYA 2005age. s. 11; Ramazan DOĞAN 2014, age. s. 87; Ahmet GÜL 2021, age. s. 105 / Katılmadığımız bir görüşe göre ise normun lafzında ''hukuka aykırı olarak'' denilmesinin herhangi bir önemi bulunmayıp, hakime hukuka uygunluk nedenlerini iyi değerlendirmesi yönünde bir vurgudan öte vaziyet yaratmamaktadır. Bkz. Muhammet Sefa ÇETİN 2021, age. s. 13.

[370] ASS'nin yasa dışı erişim başlıklı ikinci maddesinin lafzında da suçun kasten işlenebilir olması gerektiği belirtilmiştir. Yine TCK md. 243'ün gerekçesinde, ''*Sisteme, hukuka aykırı olarak giren*

Doktrinde delil olarak sunmak için bir kişinin mağduru olduğu suçların faillerinin kimliği ya da adresinin tespiti amacıyla sistemlere yetkisiz erişim gerçekleştirmesi durumunda haksızlık bilincinin oluşmayacağı belirtilmiştir.[371] Haksızlık bilinci sübjektif tipiklik içinde değerlendirilmesi gereken bir konu olduğundan, kanaatimizce bu tür bir durum her fail ve her olayın kendi özelinde değerlendirilmelidir. Yargıtay ise aynı durumu kaybolma olasılığı bulunan ve bir daha elde edilemeyeceği düşünülen deliller yönünden değerlendirmiş ve bir kararında, boşanma davasına delil olarak sunmak üzere eşinin bilgisayarına yüklediği malware üzerinden sisteme yetkisiz erişerek verileri elde eden kocayı,

> ''*... sanığın, kaybolma olasılığı bulunan mevcut delilin muhafazasını sağlamak ve boşanma davasındaki iddiasını ispat etmek amacı taşıyan eyleminde hukuka aykırı hareket ettiği bilinciyle davranmadığı, suçun yasal unsurlarının oluşmadığı ...*''

gerekçesiyle suçsuz bulmuştur.[372]

Doktrinde suçun olası kastla da işlenebileceği[373] ve ayrıca haksızlık bilincine sahip bir failin de olası kastla hareket ediyor olabileceği yönünde görüşler bulunmaktadır.[374] Olası kast failin, suçun kanuni tanımındaki unsurların gerçekleşeceğini bilmemekle birlikte, gerçekleşebileceğini öngörmesine rağmen fiili gerçekleştirmesidir. Haksızlık bilincinin bulunması gereken bu suçta, olası kast gereğince sübjektif tipikliğinin oluşumu için failin ''*yaptığının haksız olduğunu bilmemesi fakat haksız olabileceğini öngörmesi*'' ve ayrıca ''*yaptığının sisteme erişimi sağlayacağını bilmemesi fakat bunu öngörmesi*'' şartlarının birlikte mevcut olması gerekir. Böyle bir durumun gerçekleşme olasılığı ise sanıyoruz ki pek yüksek değildir. Örneğin bir sınav sırasında öğrencilerin telefonları toplanıp bir kutuya konulmuş ve sınav çıkışı öğrenciler kendininkine tıpatıp benzeyen başkasına ait bir telefonu kutudan alarak telefondaki siber uzaya erişmiş, çeşitli işlemler yapmış olabilirler. Böyle bir durumda aynı ana ekran arka planına sahip ve tuş kilidi olmayan aynı model iki ayrı telefonun varlığında, fail telefonun üzerindeki kısmi çiziklerden veya kirlerden dolayı telefonun kendisine ait olmayabileceğine dair bir şüpheye sahip olmasına

---

kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur'' denilerek özel kast/saikin gerekmediğine dikkat çekilmiş, ''*haksız ve kasten girilmiş olması suçun oluşması için yeterlidir*'' denilerek genel kast ve haksızlık bilincine vurgu yapılmıştır.

[371] Cengiz APAYDIN 2017, age. s. 82.

[372] Yargıtay 12. CD 2014/7946 E. 2014/24202 K.

[373] Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1156; Ahmet Caner YENİDÜNYA 2005, age. s. 11.

[374] Ahu Karakurt EREN 2020, age. s. 752.

rağmen bu şüphesini tescillemek için telefonun içerisini karıştırırsa, salt haksızlık bilinci yönünden bir ‘’öngörüye rağmen gerçekleştirme durumu‘’ oluşmakta fakat sisteme erişme durumu doğrudan kastla gerçekleşmektedir. Öyleyse suçun olası kastla işlenmesine yönelik teoride bir engel bulunmadığını lakin bunun pratikte gerçekleşmesinin pek olası olmadığını söylemek, konuya dair mantıklı bir açıklama olacaktır.

Bilişim sistemine yetkisiz erişim suçunun sübjektif tipikliği yönünden faillerin bilişim sisteminin varlığına ve eylemlerinin bu yapıya erişmeye sebep olacağına dair bilinçlerinin yani özünde bilişim teknolojilerine dair bilgilerinin, hedef sistemler ve hareketlerin gerçekleştirilme şekilleri bakımından her somut olayda ayrı ayrı değerlendirilmesi gerekir. Zira çok farklı bilişim sistemlerine çok farklı yollardan erişilebilmektedir. Örneğin bugün için Türk toplumundaki teknolojiden aşırı izole istisnai bireyler haricindeki herkes bilgisayar, cep telefonu, tablet ve sair klasik bilişim sistemlerinin ne olduğunun ve bunların nasıl kullanıldığının bilincindedir. Lakin bunların ne işe yaradığını bilmeyen bir kişinin, yaptığı hareketin kendisini sisteme eriştireceğini öngörebilmesi dahi imkansız olabilir. Bu durumun özellikle yeni nesil IoT sistemler veya sıra dışı tasarıma sahip sistemler yönünden gündeme gelmesi mümkündür.

Bireylerin sinyalleri kendi wi-fi kartına kadar varan bir wi-fi bağlantı noktasına yetkisiz olarak bağlanılmaması gerektiğinin bilincinde olduğunu söylemek de pekala mümkündür. Örneğin toplumun çoğu üyesi, ‘’GFB‘’ SSID’sine sahip bir bağlantı noktasına ‘’1907‘’ şifresini girerek erişmeye çalışmaması, şans eseri erişse bile anında bağlantıyı koparması gerektiğini bilecektir. Ancak ilk defa torununun bilgisayarını kullanan yaşlı biri, rastgele bilgisayarı kurcalarken adeta bir bulmaca çözdüğünü sanarak GFB’nin altına 1907 yazarak ağa yetkisiz olarak bağlanabilir.

Esasında bilgisayar, cep telefonu ve internet kullanan bireylerin dahi öngöremeyeceği, somut olayda öngörmediği(*taksir*) ya da öngörse bile istemediği(*bilinçli taksir*) durumların varlığı da gündeme gelebilir. Hacking yöntemlerinde, yukarıda detaylı olarak açıklandığı üzere güvenlik açıklarından yararlanılabilmekte ve bazen de hedef sisteme gönderilen anlamlandırılamaz veri paketleri sayesinde hedef sistemdeki yazılım manipüle edilerek, sistem yetkisiz olarak erişilebilir kılınmaktadır. Hackingde bu durumlar bilinçli olarak yaratılıyor ise de pekala sıradan bir internet kullanıcısının, rastgele girdiği bir URL bağlantısıyla SQL manipülasyonu yaratması ve sunucudan erişememesi gereken verileri çekmesi

mümkün olabilir. Yetkisiz olarak kalmaya devam etme yönünden de benzer durumların yaşanması mümkündür. Örneğin hedef sisteme bağlanma ve kontrol etme imkanı sunan bir yazılımın her iki sistemde de eş biçimde çalıştırılması durumunda, kişi ağ üzerinden diğer sistemi kolayca kontrol edebilmektedir. Böyle bir bağlantıyı kullanan teknik destek elemanı hedef sisteme uzaktan erişim sağlayarak karşı tarafın rızası dahilinde belirli işlemler gerçekleştirebilir ve bilahare bağlantıyı kesebilir, kesmez ise yetkisiz olarak kalmaya devam etme durumu meydana gelecektir. Eğer teknik destek elemanı uygulama yazılımı ekranındaki ‘’X-çıkış‘’ butonuna basıldığında arka planda bağlantının süreceğini bilmiyorsa, bu şekilde sistemde yetkisiz olarak kalmaya devam eden ve iki sistem arasında veri alış verişini sürdüren elemanın kastının varlığından söz edilemeyecektir.

3.2.2.2. Yapay Zeka Kullanımı ve Sübjektif Sorumluluk Sorunu

Yapay zeka yazılımların bilişim sistemleri içerisinde kullanımı veya bu yazılımlar ile donanımların entegre biçimde otonom olarak hareket ettiği robotların, araçların yahut sair makine sistemlerinin kullanımı günümüzde oldukça yaygındır ve bu kullanım oranı her geçen gün hızla artmaya devam etmektedir. Yapay zeka teknolojileri sabit hesaplamalar üzerine kurulu algoritmalara göre değil, makine öğrenimi/derin öğrenme teknikleri kullanılarak[375] algoritmadaki sabit sınırların ötesinde hesaplamalar yapılması ve uygun sonuçların üretilebilmesi amacıyla kullanılır. Bu sebeple yapay zeka teknolojiler önceden belirlenmiş sonuçları değil, ancak ‘’belirli bir çerçevede öngörülebilir‘’ sonuçları üretirler. Örneğin bir otonom aracın hangi nesneleri gördüğünde temastan kaçınmak için ani fren yapması gerektiği genel çerçevesiyle yazılımına işlenir/öğretilir, birebir öğretilmemiş veya öğretilmiş kalıplara uymayan nesnelerle karşılaştığında ise yazılımlar duruma en uygun sonucu üretecek şekilde tasarlanabilir. Bu sayede de yolda ağaç kostümüyle yürüyen bir yayanın varlığında aracın bunun bir ağaç olmadığını, hareket ettiğini ve biraz sonra önüne çıkacağını fark ederek ani fren yapması mümkün olur. Doktrinde bu tip davranışların da öngörülebilir olmadığı belirtilmekte[376] ise de kanaatimizce zararlı

[375] ‘’*Bu yapılar insan beyninin öğrenme metodunu taklit ederek elde ettiği verilerden yeni verilerin üretilebilmesini sağlayan yazılımlardır*.‘’ Pınar BACAKSIZ ve Seda YAĞMUR SÜMER (2021), *Robotlar, Yapay Zeka ve Ceza Hukuku*, Adalet, Ankara, s. 25.

[376] ‘’*Yapay zekalı bir makinenin davranışı, uygun bir davranış modelinin yazılımına dahil edilmediği bir durumla karşı karşıya kaldığında ve ‘’tecrübeye’’ dayalı olarak otonom şekilde belirli bir eyleme karar verdiğinde, öngörülebilir nitelikte değildir*.‘’ Zeynel T. KANGAL (2021), *Yapay Zeka ve Ceza Hukuku*, Oniki Levha, İstanbul, s. 28.

sonuçların minimize edilmesi için sisteme belirli veri yüklemeleri, öğretimler ve testler yapıldığında, sistemin üretilenin ötesinde çıkarımlar yapması bu öğretilen veri havuzu üzerinden gerçekleşeceğinden, sonuçlar bu çerçeve içerisinde öngörülebilirdir. Öngörülebilen bir netice pekala bilinebilir, istenebilir ve bu şekilde kasten gerçekleştirilebilir olduğundan, kanaatimizce bu tür teknolojilerin varlığında yetkisiz erişim suçunun sübjektif tipikliğinin oluşması mümkündür.

Yapay zeka teknolojisinin bu önceden belirlenmiş veri havuzu çerçevesinde kendisini geliştirebilmesi, müspet amaçlar için de menfi amaçlar için de sağlanabilir. Aynı şekilde hangi amaçla olursa olsun, bu şekilde hareket alanı sınırlandırılmış bir yapay zeka teknolojisinin suçta bu özellikleri bilinerek araç olarak kullanılması da mümkündür. Örneğin bu amaçla üretilen bir yapay zekaya sahip SİHA'nın insan öldürmede araç olarak kullanılması mümkündür ve bu gibi durumlarda fail açısından neticenin öngörülebilirliğine yönelik bir sorun oluşmaz. Bu sebeple yetkisiz erişim suçuna konu seçimlik hareket/neticeleri gerçekleştirmek zaten amacı olan yazılımların suçta kullanımı, sübjektif sorumluluk nazarında bir tartışma yaratmayacaktır.[377]

Bir yapay zeka teknolojisinin gerçekleştirmesi istenilen sonuçlar bakımından, yapay zekanın veri havuzunu kendisinin oluşturması ve bu rastgele seçilecek veriler üzerinden kendisini geliştirmesine yönelik deneysel bir teknolojinin varlığında ise üretilen sonuçlar belirli bir öngörülebilirlik çerçevesi içerisinde değerlendirilemez. İşte öngörülebilir olmayan bu tür yapay zeka teknolojileri, kast ve hukuka aykırılık bilinci gerektiren yetkisiz erişim suçu yönünden ve sair her türlü suça dair sübjektif sorumluluğun oluşumu bakımından sorun arz etmektedir. Özel hukukta bu durum kolektif sorumluluk normlarının varlığı ve doktrinde de yapay zekanın öngörülemez zararlarında kolektif sorumluluğun gündeme geleceği yönündeki çoğunluk görüşü ile aşılmıştır.[378] Neticenin sübjektif olarak öngörülebilir olmasının arandığı ve böyle bir durum yok ise taksir derecesinde dahi bir sorumluluğun doğmayacağı Türk ceza hukuku yönünden ise ne objektif sorumluluk ne de kolektif sorumluluğa dair çözümler üretmek mümkün değildir.[379]

---

[377] Zeynel T. KANGAL 2021, age. s. 92-93.

[378] Doktrindeki görüşlere dair kısmi külliyat için bkz. Alp ÖZTEKİN (2021), *Türk İnternet Hukuku*, Seçkin, Ankara, s. 354, 355, 356 vd.

[379] Uygun sebep ve şart teorisi + objektif isnat edilebilirlik yönünden de bu tür öngörülemez neticeler, illiyet bağı açısından sorun oluşturacaktır. Karma nedenselliğe göre bu sorun aşılabileceğinden, işbu tez kapsamında bu sorunun değerlendirilmesi sübjektif tipiklik özelinde yapılmıştır. Nedensellik bağının kesileceğine dair benzer görüşler için bkz. Enes KÖKEN (2021), ''Yapay Zekanın Cezai Sorumluluğu'', *Türkiye Adalet Akademisi Dergisi*, C. 12, S. 47, ss. 247-286, s. 268 / Yapay zeka konusunda ceza hukuku yönünden mevcut sorumluluk teorilerinin yetersizliği üzerine ayrıca bkz.

Yapay zeka hukuken bir kişi olarak kabul edilmediği ve fail konumunda bulunamayacağı için bu tür teknolojilerden doğan zararlardan ceza hukuku boyutuyla üreticiler, kullanıcılar ve sair ilgililer sorumlu tutulabilecektir.[380] Lakin makine öğrenimi/derin öğrenme tekniklerinde sistemin öğrenme + akıl yürütme ile sergilediği otonom davranışlardan dolayı herhangi bir suçun objektif tipikliğine giren bir neticenin doğması durumunda, üreticinin dahi bu neticeden ceza hukuku gereğince sorumlu tutulabilmesi çoğu zaman sübjektif sorumluk şartı sebebiyle mümkün olamamaktadır. Doktrinde Hilgendorf bu durumu ‘’sorumluluğun erimesi‘’ olarak adlandırmaktadır.[381] Örneğin web üzerinde veri madenciliğinde kullanılan bir yapay zeka teknolojisi, pek çok noktaya erişmek ve buralardaki verileri taramak amacıyla kullanılır. Kendisine önceden öğretilmiş veriler üzerinden yola çıkarak ve pekala benzer durumları da kendisi öğrenerek surface web ve deep web'deki pek çok noktaya erişim sağlayan yazılım, sahip olduğu yeteneklere ve kullanım şekline göre çeşitli sonuçlar doğurabilir.

Evvela bu yazılım belirli bir öngörülebilirlik içerisinde hareket edecek şekilde ve hukuka uygun kullanımlar hedeflenerek oluşturulmuş fakat beklenmeyen bir sonuç doğurarak yetkisiz erişim gerçekleştirmiş olabilir. Doktrinde bu tür durumlara dair üretici ve kullanıcılar her türlü önlemi almış ve taksir derecesinde dahi bir özensizlik söz konusu değilse, cezai açıdan bir sorumluluğun doğmayacağı belirtilmektedir.[382] Aynı şekilde her türlü önleme rağmen önlenemez neticelerde, meseleye objektif isnat edilebilirlik nazarında bakan ve bu durumların izin verilen risk olarak görülmesi gerektiğini belirten görüşler de mevcuttur.[383] Böyle bir durumda üreticilerin taksirle sorumluluğunun gündeme geleceğine dair zıt yönde görüşler de doktrinde dile getirilmektedir.[384]

Thomas C. KING, Nikita AGGARWAL, Mariarosaria TADDEO ve Luciano FLORİDİ (2021), ‘’Yapay Zeka Suçu: Öngörülebilir Tehditleri ve Çözüm Yılları Üzerine Disiplinler Arası Bir Analiz‘’, Çev: Hasan Dursun, İçinde, *Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler*, Proje Yöneticisi: Kayıhan İçel, Ed. Yener Ünver, ss. 248-289, Seçkin, Ankara, s. 253, 254, 259, 273, 274.

[380] Pınar BACAKSIZ ve Seda YAĞMUR SÜMER 2021, age. s. 163; Enes KÖKEN 2021, age. s. 269.

[381] Eric HİLGENDORF (2021), ‘’Endüstri 4.0'da Sorumluluğun Erimesi ve Kendi Kendine Öğrenen Sistemler-Ceza Hukuku Açısından Sorun Özeti‘’, Çev: Enis Tiz, İçinde, *Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler*, ss. 47-61, Seçkin, Ankara, s. 58.

[382] Eric HİLGENDORF 2021, age. s. 53, 54.

[383] Zeynel T. KANGAL 2021, age. s. 106.

[384] Enes KÖKEN 2021, age. s. 269.

Eğer beklenmeyen bir durumun olmaması için üretim aşamasında yapılabilecek tüm standart uygulamalar gerçekleştirilmiş ve testler yapılmış ise meydana gelen sonucun üreticiler açısından sübjektif olarak öngörülebilir olmadığını söylemek gerekir. Aynı şekilde test edildiğine ve bu şekilde piyasaya sürüldüğüne güvenerek yazılımı kullanan bir kişinin de hataya dair istisnai şekilde edinebildiği bir bilgisi yoksa, sübjektif olarak neticeyi öngörebilmesinin imkansız olacağını söylemek gerekir. Bu sebeple kanaatimizce bu tür durumlarda herhangi bir fail açısından kast ya da taksir gündeme gelemeyeceğinden, suçun sübjektif tipikliği oluşmayacak ve beraat kararı verilecektir.

İkinci olarak belirli bir öngörülebilirlik içerisinde hareket edecek şekilde tasarlanmış olan yazılımın, şifreli veri tabanlarına ve içeriklere erişmesi de istenmiş, brute force saldırısı yaparak bu şifreli alanların içeriğindeki verileri de taraması yazılımın yetenekleri arasına eklenmiş olabilir. Böyle bir durumda bu yazılım, kullanım amacı doğrultusunda yetkisiz erişimler gerçekleştirecektir. Suç aleti olan yazılımın bu tür bir kullanımında ne üretici ne de kullanıcılara dair sübjektif sorumluluk yönünden bir sorun oluşmayacak, kasta bağlı sorumluluk doğacaktır. Böyle bir durumda şüphesiz ki üretici eğer bu yazılımı hukuka uygun şekilde kullanılması amacıyla üretmişse fiili hukuka uygun olabilecektir.[385]

Üçüncü olarak belirli bir öngörülebilirlik içerisinde hareket edecek şekilde tasarlanmadan ve buna dair gerekli testler de gerçekleştirilmeden piyasaya sürülmüş bir yazılım, web içeriklerini taramak yerine çeşitli ağlara bağlanmaya ve ağlardaki sistemler içerisindeki gömülü verileri de taramaya başlamış ve bu sayede pek çok yetkisiz erişim gerçekleştirmiş olabilir. Doktrinde böyle bir durumda üreticilerin neticeden olası kastla sorumlu olacakları yönünde görüşler mevcuttur.[386] Bu durumu bilerek böyle deneysel/sınırlandırılmamış yapay zeka teknolojilerini kullananların ise daima en aşağı taksirle sorumlu olacakları ve bu durumda bir taksir karinesinin söz konusu olacağı da zikredilen görüşler arasındadır.[387] Yine doktrinde bu durumda kullanıcılar açısından taksir karinesinden bahsetmeyen lakin kullanıcıların taksirli sorumluluklarına gidilebileceğini belirten görüşler de mevcuttur.[388]

[385] Bu durum ayrıca md. 245/A'nın da tipikliği içerisinde kalacaktır.
[386] Zeynel T. KANGAL 2021, age. s. 99.
[387] Zeynel T. KANGAL 2021, age. s. 104.
[388] Pınar BACAKSIZ ve Seda YAĞMUR SÜMER 2021, age. s. 168.

Olası kast için bir ‘’öngörülen neticeye karşı kayıtsız kalma‘’ şartı gerektiğinden ve taksir için de neticenin sübjektif olarak öngörülebilir olması zaruri olduğundan, bu noktada yapılan genellemelere katılmak mümkün değildir. Böyle bir durumda eğer hem üretici taraf hem de kullanıcı tarafın neticeyi sübjektif olarak öngörebilmesi mümkün değil ise sübjektif sorumluluk oluşamaz. Bu tür deneysel uygulamalarda da zaten netice kuvvetle muhtemel öngörülebilir değildir. Bu tür durumlarda cezasızlığın önüne geçilebilmesi için yapılabilecek tek şey, spesifik maddi ceza normları oluşturulmasıdır. TCK incelendiğinde bu yönde spesifik bir norm olmadığı, 7223 s. Ürün Güvenliği ve Teknik Düzenlemeler Kanunu[389], 4703 s. Ürünlere İlişkin Teknik Mevzuatın Hazırlanması ve Uygulanmasına Dair Kanun[390] ile 6502 s. Tüketicinin Korunmasına Dair Kanun[391] gibi üretici denetimine dair düzenlemelerde de spesifik olarak yazılımlara dair hükümler bulunmadığı ve cezai bir normun da mevzuatta yer almadığı görülmektedir.[392] Öyleyse sonuçları sınırlandırıcı testler yapılmadan yazılımları kullanıma sunan ve bu durumu bilerek kullananlar hakkında TCK md. 175-176-177 normlarına benzer spesifik suç normlarının oluşturulması gerekmektedir.

Dördüncü ihtimalde ise analiz yazılımını kullanan kişi yazılımın çalışmasını izlediği sırada, yazılımın bu tür yetkisiz erişimler gerçekleştirmek için ağlara bağlanmaya ya da brute force saldırıları gerçekleştirmeye çalıştığını fark etmesine rağmen buna kayıtsız kalabilir. Doktrinde haklı olarak bu gibi durumlarda kullanıcı yönünden ihmal suretiyle suçun işlenebileceği ve sorumluluğun gündeme geleceği belirtilmektedir.[393]

[389] Yayımlandığı Resmî Gazete: Tarih: 12/03/2020 Sayı: 31066
[390] Yayımlandığı R. Gazete: Tarih: 11/7/2001 Sayı: 24459
[391] Yayımlandığı Resmî Gazete: Tarih: 28/11/2013 Sayı: 28835
[392] Otonom araçlar ile ilgili düzenlemeler getiren Motorlu Araçlar ve Römorkları ile Bunlar için Tasarlanan Aksam, Sistem ve Ayrı Teknik Ünitelerin Genel Güvenliği ve Korunmasız Karayolu Kullanıcılarının ve Yolcuların Korunması ile İlgili Tip Onayı Yönetmeliği'nde ise AB ve BM regülasyonlarına yollama yapılarak, dolaylı yoldan otonom araçlara dair bir güvenlik önlemi getirilmiştir. Lakin dayanak kanununda yapay zekanın test edilmemesinden doğan zararlara yönelik bir ceza normu bulunmamaktadır.
[393] Zeynel T. KANGAL 2021, age. s. 96; Philip TARPLEY ve Steven D. JANSMA (2016), *Autonomous Vehicles: The Legal Landscape In The US*, Norton Rose Fulbright, https://www.nortonrosefulbright.com/en/knowledge/publications/2951f5ce/autonomous-vehicles-the-legal-landscape-in-the-us, (ET: 02.03.2022), s. 13.

3.3. SUÇUN HUKUKA AYKIRILIK UNSURU

3.3.1. Suç Tipi ile Bağdaşabilen Hukuka Uygunluk Sebepleri[394]

Doktrinde yetkisiz erişim suçu ile bağdaşabilen hukuka uygunluk sebeplerinin kanun hükmünü icra, rıza ve hakkın kullanılması olduğu yönünde görüşler[395] bulunduğu gibi yalnızca kanun hükmünü icra ve rızanın bu suç ile bağdaşabileceği[396] yönünde görüşler de mevcuttur. Bir kısım görüş ise yalnızca kanun hükmünü icranın bu suç yönünden hukuka uygunluk sebebi teşkil edebileceğini belirtmektedir.[397] Kanaatimizce yetkisiz erişim suçu ile TCK'nın lafzında yer alan tüm hukuka uygunluk sebeplerinin bağdaşması mümkün olup, aşağıda bu konudaki değerlendirmeler spesifik başlıklar altında açıklanmıştır.

3.3.1.1. Hakkın Kullanılması

Yetkisiz erişim suçu nazarında meşru bir hakkın kullanılmasının hukuka uygunluk sebebi teşkil ediyor olması, genel olarak sözleşmeden veya sair bir hukuki ilişkiden doğan ve sistem üzerinde erişim yetkisi sağlayan hakların kullanılması şeklinde tecelli edecektir. Doktrinde basın hürriyetinin kapsamında sistemlere erişilerek haber değeri taşıyan bilgilere ulaşılabileceği belirtilmiş[398] ise de bu yöndeki Anayasal hürriyetlerin kullanımının ilgili suçta bir hukuka uygunluk sebebi teşkil edebileceğini düşünmüyoruz. Aksine, bir basın mensubu eğer haber elde edebilmek için bir bilişim sistemine yetkisiz olarak erişir ise suç işlemiş olacaktır.[399]

TMK'da yer alan velayet hakkı gibi bir kısım spesifik hakların kullanımının da bilişim sistemine erişim yetkisi verebilmesi mümkündür. Örneğin velayet hakkı sahibi bir babanın, bu hakkını kötüye kullanmadığı sürece on yaşındaki çocuğunun bilgisayarına gerekiyorsa zorla erişmesi ve kontrol etmesi mümkündür. Kanaatimizce kınanabilirlik içerisinde değerlendirilmesi gereken bir mesele olan, ''*özel kişilerin*

[394] Türk hukuk doktrininde, TCK'da yazılı olan hukuka uygunluk sebeplerinin neler olduğu konusunda bir fikir birliği bulunmayıp, bazı durumlar bir kısım yazar tarafından kınanabilirlik/kusurluluk içerisinde değerlendirilirken, aynı durumları hukuka uygunluk sebebi olarak değerlendirmiş görüşler de mevcuttur. İşbu tez kapsamında (*yazılı*)hukuka uygunluk sebepleri, CMK md. 223/3'ün kusurluluğa dair lafzı ile TCK'nın ''ceza sorumluluğunu kaldıran ve azaltan nedenler'' başlığı altındaki düzenlemeleri birlikte değerlendirilerek; hakkın kullanılması, kanun hükmünü icra, meşru savunma ve ilgilinin rızası olarak kabul edilmiştir.

[395] Murat Volkan DÜLGER 2022, age. s. 299, 300.

[396] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 964; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 245.

[397] Doğan SOYASLAN 2020b, age. s. 663.

[398] Büşra ÖZÇELİK 2019, age. s. 82, 83.

[399] Benzer görüşler için bkz. Murat Volkan DÜLGER 2022, age. s. 302.

başka zaman toplanamama ihtimali bulunan delilleri elde etmesi'' durumu doktrindeki bir kısım görüşlerde hak arama hürriyetinin kullanılması özelinde değerlendirilebildiğinden,[400] TCK md. 243'ün ve bilişim sistemlerine yetkisiz erişimin delil elde etmeye yönelik fiiller boyutuyla da değerlendirilmesi tartışılabilir.

Mülkiyet ve zilyetlik hakkının ise bu suç yönünden direkt olarak bir hukuka uygunluk sebebi teşkil etmesi mümkün değildir. Zira pratikteki işleyiş de böyle olduğu üzere, kişiler maliki oldukları sistemleri tamamen başkalarına tahsis edebilmekte, sistemlerin zilyetleri de bunları veri boyutuyla başkalarına tahsis edebilmekte ve malik ile zilyet olan bu kişiler sistem içeriğine ''erişmemeyi'' de bu tahsis ile birlikte taahhüt etmektedirler. Bu noktada önemli olan husus mülkiyet ya da zilyetlik değil, sisteme erişim yetkisidir. Mülkiyet ve zilyetlik noktasında değerlendirilmesi gereken esas mesele ise çöpe ya da bir köşeye atılmış yahut bulunmuş bilişim sistemlerinin durumudur. Doktrinde sistemi çöpe atan kişinin artık sistem/veriler[401] üzerindeki hak sahipliğinin biteceği, terk edilmiş bir mal üzerinde bir mülkiyetin bulunmayacağı ve herkesin bu mallar üzerinde tasarruf sahibi olabileceği belirtilmektedir.[402] Gerçekten de eğer bir kimsenin bilgisayarını çöpe attığı konusunda bir şüphe yoksa, 4721 s. Türk Medeni Kanunu[403] md. 767 gereğince bunu zilyetliğine geçiren kişi malik sayılacaktır. Bulunan eşyalar bakımından ise TMK'nın 769 ve 770. maddelerinde bir kısım şartlar sıralanmış, 771. maddede ise şartlar gerçekleştikten sonra beşinci yılın sonunda mülkiyet hakkının bulan kişiye geçeceği düzenlenmiştir. Ancak bilişim sistemleri yönünden kanaatimizce TMK'ya ek bir düzenleme eklenmeli ve ne şart altında olursa olsun, sahipsiz olduğundan şüphe edilen sistemlerin içeriğine erişilmeden her halükarda kolluk birimlerine teslimi, belirli bir süre sonra sahibi bulunamayan sistemlerin ise bilahare BTK yahut EGM bünyesinde oluşturulacak birimler tarafından içeriğindeki veriler geri döndürülemez biçimde silinerek(*wipe*) sıfırlanması gerekmektedir. Zira bilişim sistemleri sokakta ya da çöpte bulunan sıradan bir eşya olmayıp, içerisindeki verilere erişim son derece sakıncalı sonuçlar doğurabilir.

Hakkın kullanılması hukuka uygunluk sebebi noktasında, işverenlerin ya da bu yetkiye sahip ağ yöneticisi çalışanların veya dışarıdan BT hizmeti alınıyorsa bu servis

---

[400] Fatih BİRTEK (2017), *Ceza Muhakemesinde Delil ve İspat*, Adalet, Ankara, s. 324.
[401] Nurullah KUNTER, Feridun YENİSEY ve Ayşe NUHOĞLU (2013), *Açıklamalı Ceza Muhakemesi Kanunu Cilt 1*, Beta, İstanbul, s. 1305, 1306.
[402] Ahmet KILIÇ (2018), ''Kaybolmuş veya Hata Sonucu Ele Geçmiş Eşya Üzerinde Tasarruf Suçu'', *Yıldırım Beyazıt Hukuk Dergisi*, C. 3, S. 2, ss.1-35, s. 9.
[403] Yayımlandığı Resmî Gazete: Tarihi: 8/12/2001 Sayı: 24607

sağlayıcının, işçilerin kullanımındaki sistemlere erişebilmesi durumu da açıklanmalıdır. Evvela belirtmek gerekir ki bir iş yeri ağı oluşturuluyor ve bu ağda en az bir yönetici ile birden fazla sınırlı işlem yapabilen sair sistemlerin yer alması isteniyorsa, switch ve sair noktalara bağlı monitör sistemler ya da her bir sisteme yüklenen yazılımlar vasıtasıyla hem ağ trafiğinin hem de sistemlerin iç işleyişinin takip edilmesi zarurettir. Hukukumuzdaki pek çok norma göre gerek kişisel veriler yönünden gerekse direkt olarak ağ ve sistem güvenliğine dair bir siber güvenlik uygulaması oluşturulması da zaten zorunlu kılınmıştır.

Sistemlerin yalnızca işyerinde işlerini görmeleri için çalışanlara kullandırıldığı durumlarda, istisnai durumlar haricinde sistemler üzerindeki tüm yetkiler işverenindir. İstisnai durumlar ise kritik veri tabanları ya da uygulamalara belirli özel yetkilerle erişilebilmesinin mevzuat gereği şart koşulduğu vaziyetlerdir. Bu tür istisnai durumlar dışında işverenin tüm yetkileri esas olarak kendisine ait olan bir sisteme her daim yetkili olarak erişebileceği açıktır. Bu açıklamalar hem bilgisayar ya da telefon gibi cihaz şeklindeki bilişim sistemleri hem de mail hesapları için geçerlidir. Zira iş/şirket mailinin işveren tarafından denetimi sırasında da işveren esasında kendisinin yetkili olduğu fakat bir işi gördürmek için çalışanlarına kullandırdığı bilişim sistemlerine/sunuculara erişmektedir. Öyleyse işverenin bilişim sistemlerinin içeriğine erişerek denetimler yapması, TCK md. 243/1 bağlamında ‘’*yetkili olması ve bu yetkiyi çalışanlarına devretmemiş olması*‘’ gereğince hukuka uygundur. İşveren sistemlere erişim yetkisini iş sözleşmesi, sistemlerin kullanımına dair sözleşmeler ve sair vasıtayla kısıtlamış ise şüphesiz ki kısıtlanan noktalarda bir erişim yetkisinden söz edilemeyecektir. Her ne kadar işçinin işyerindeki bilgisayarı ya da iş için kullandığı telefonunu özel hayatına yönelik kullanmaması gerekiyor ise de sistem içerisindeki kişisel veriler veya gizli haberleşmelerin öğrenilmesi yetkisiz erişim suçunun tipikliği içerisinde olmadığından, işverenin hukuka uygun biçimde eriştiği sistem içerisindeki bilgileri öğrenmesi durumunda oluşabilecek suçlar, TCK md. 243’ün alanı dışında kalacaktır.[404]

[404] Doktrinde her ne kadar Yargıtay kararına da atıf yapılarak sistemlere erişimlerin işverenin denetim yetkisinden kaynaklandığı belirtilmiş ise de kanaatimizce bu tür bir denetim yetkisi esas olarak kişisel veriler veya haberleşmenin gizliliği yani sistemlerdeki ‘’bilgilerin öğrenilmesi‘’ noktasında bir hukuka uygunluk sebebi teşkil edebilir. Doktrin görüşleri için bkz. Meral EKİCİ ŞAHİN ve Irmak KORUCULU 2019, age. s. 607 ve aynı kaynakta: Yargıtay 9. HD 2010/447 E. 2010/37516. / Bu tür durumlarda çalışanlara bilgilendirme yapılmaz ise haberleşmenin gizliliği, özel hayatın gizliliği ya da kişisel veriler yönünden bir kısım suçların gündeme gelmesi söz konusu olabilir. Zira iş için kullanılması şart koşulmasına ve sözleşmede de özel işler için kullanılamayacağı yazılı olmasına rağmen, işverenin bir bilgisayar ya da mail içeriğindeki tüm bilgileri işveren sıfatı gereği öğrenebilmesi mümkün değildir.

Spesifik olarak bazı kanuni düzenlemelerin, sistemlere erişim yönünden gerçek ya da tüzel kişilere bazı haklar vermesi de mümkündür. Örneğin 5369 s. Evrensel Hizmet Kanunu[405] gereğince elektronik haberleşme hizmetlerinin kullanılması, erişim sağlayıcı şirketlerin keyfi rızalarına bağlı olmayıp, bedelini ödeyen herkesin bu evrensel hizmete dahil olabilmesi gerekir. Böyle bir durumda gerçekleşen abonelik sözleşmesi gereğince internet omurgasına erişimin kanaatimizce rıza değil, hakkın kullanılması hukuka uygunluk sebebi çerçevesinde değerlendirilmesi gerekir. Elektronik haberleşmeye dayalı evrensel hizmetlerde, kullanıcılara ek olarak işletmeci erişim sağlayıcılar yönünden de 5809 s. Elektronik Haberleşme Kanunu[406] md. 15-16-17 vd. ile Erişim ve Arabağlantı Yönetmeliği'nde ve bu yöndeki BTK kararlarında benzer düzenlemeler mevcuttur. Bu düzenlemelere göre şartları bulunuyor ise omurgayı işleten erişim sağlayıcının bu omurgayı, omurga altyapısını kullanarak hizmet vermek isteyen üçüncü taraflar ile ortak erişime açması şart tutulmuştur.[407] Bu yönde BTK'nın onayı gerekebiliyor ise de kamu yararı ve normatif şartların oluşumu

Libert v. France kararında AİHM, iş sözleşmesi yahut ilgili işyeri belgelerinde aksi bir durum yazılı değil ise işverenin denetim yetkisi kapsamında ''özel'' nitelemesi ile işaretlenmeyen veri dosyalarının incelenebileceğini, iş bilgisayarında normal şartlarda özel bilgilerin bulunamayacağını ve bunun özel hayatın gizliliği kapsamında kalmayacağını belirtmiştir. Öyleyse bir işçinin ''özel'' etiketi ile adlandırdığı klasörlerin ya da mail başlıklarını taşıyan maillerin açılamayacağını söylemek gerekir. Her ne kadar bu tür bir vaziyet haklı olarak iş sözleşmesinin feshini gerektiriyor ise de bu tür verilerin içeriği okunmadan silinmesi doğru olacaktır. Aksi bir işlem gerçekleştirilmek isteniyor ise mutlaka buna dair bir onamın sözleşmede veya işçinin haberdar olması gereken bir belgede yazılı olması şarttır. AYM'nin 2013/4825 başvuru numaralı Ömür Kara ve Onursal Özbek başvurusuna dair verdiği kararda da sözleşme ve işyeri belgelerinde bu tür inceleme ve denetimlerin yapılabileceğinin açıkça yazılı olduğuna da dikkat çekilerek, özel hayat ve haberleşmenin gizliliğine dair haklara bu noktada halel gelmeyeceği zikredilmiştir.

[405] Yayımlandığı Resmî Gazete: Tarih: 25/6/2005 Sayı: 25856

[406] Yayımlandığı Resmî Gazete: Tarih: 10/11/2008 Sayı: 27050 (Mükerrer)

[407] ''*5809 sayılı Elektronik Haberleşme Kanunu'nun 60'ncı maddesinin birinci fıkrasına, Bilgi Teknolojileri ve İletişim Kurumunun Denetim Çalışmalarına İlişkin Yönetmelik'in 10'uncu maddesinin ikinci fıkrasına, Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği'nin 10'uncu maddesine ve ilgili diğer mevzuata istinaden; 31.12.2019 tarihli ve 2019/DK-SRD/338 nolu Kurul Kararı ile onaylanarak yürürlüğe giren "Toptan Sabit Yerel ve Merkezi Erişim Pazarları Analizi" kapsamında Türk Telekomünikasyon A.Ş. (Türk Telekom)'ye getirilen fiziksel şebeke unsurlarına erişim sağlama yükümlülüğüne aykırılığı olarak, Turknet İletişim Hizmetleri A.Ş.'nin 2014 yılında Türk Telekom'un altyapısında kurduğu fiber kablolarına İstanbul ili Kadıköy ilçesi sınırları içerisinde Karakolhane Caddesi ile Duatepe Sokak kesişiminde yer alan bir menholde ilave bağlantı yapmaya ilişkin 01.04.2020 tarihli erişim talebini haklı bir gerekçe olmaksızın reddetmesi/geciktirmesi nedeniyle Türk Telekomhakkında; Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği'nin "Erişim ve arabağlantıya ilişkin ihlaller" başlıklı 10'uncu maddesinin birinci fıkrasının (a) bendinde yer alan; "a) İşletmecinin; 1) Erişim sağlamaya ilişkin yükümlülüklerini, ... yerine getirmemesi veya haklı bir neden olmaksızın geciktirmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır." Hükmü... ölçütler çerçevesinde; 2019 yılı net satış tutarı (10.599.714.387,24₺)'nın yüzbinde beş (%0,005)'i oranında idari para cezası uygulanması hususuna karar verilmiştir.*'' Bilgi Teknolojileri ve İletişim Kurulu Kararı, Karar Tarihi: 27.07.2021, Karar No: 2021/İK-ETD/198.

durumunda BTK'nın onay vermesi gerektiğinden, bu erişim durumu bir hakkın kullanılması olarak değerlendirilmelidir.

3.3.1.2. Kanun Hükmünü İcra

3.3.1.2.1. Arama

Bir kanun hükmünü icra etmek amacıyla bilişim sistemlerine yönelen aramalar, TCK md. 243/1 nazarında meydana gelebilecek en somut hukuka uygunluk sebeplerinden biridir. Hukukumuzda bu tür bir aramayı düzenleyen temel norm CMK md. 134 olup, maddede genel olarak mahallinde ve el konularak yapılan aramalar düzenlenmiştir. Aşağıda CMK md. 134'e ek olarak, dünyada muadil uygulamaları bulunan uzaktan arama prosedürlerinin Türk hukuku yönünden mümkün olup olmadığı da tartışılmıştır.

3.3.1.2.1.1. Mahallinde ve El Konularak Arama(*CMK md. 134*)

CMK md. 134'e göre bulunduğu konum tespit edilmiş olan bilişim sistemlerinin, sistemlere yapılan fiziki müdahaleler yoluyla aranması mümkündür. Bu aramalar ya sistemin bulunduğu yerde ya da ilgili normdaki şartlar mevcut ise sistemlere el konulduktan sonra adli bilişim birimlerinde yapılır. Örneğin bu yöntemde TOR ağı üzerinde kırmızı reçeteli ilaçların satıldığı bir onion sitesindeki suça konu verileri barındıran sunucunun IP ve port bilgisi tespit edilmiş olsa bile bu sunuculara ağ üzerinden erişilerek arama yapılamaz. Trafik bilgisi üzerinden sunucuların fiziki konumları tespit edildikten sonra mahallinde bu sunucuların aranması veya el konulduktan sonra aramanın tatbiki gerekir. Nihayetinde arama kararı ve kararın icrasına dair uygulama hukuka uygun ise kanun hükmünü icra sebebiyle bilişim sistemine hukuka uygun olarak erişilmiş olacaktır.

3.3.1.2.1.2. Uzaktan Aramanın Türk Hukuku Yönünden Olanaklılığı Sorunu

Uzaktan arama, bilişim sistemlerine fiziki müdahaleler yoluyla değil, ağ bağlantısı üzerinden gerçekleştirilen erişimler vasıtasıyla yapılan aramalardır. Günümüzde internet trafiği küresel bir boyutta olduğundan ve tek suça konu sistemler dünyanın pek çok noktasına dağılmış halde bulunabildiğinden, temel haklar boyutundaki dezavantajlarına rağmen adli bilişim ve delillerin elde edilebilmesi açısından uzaktan aramalar faydalı olabilir. Lakin bu faydanın temel hak ve

hürriyetlerin ihlali karşısında baskın olabilmesi için sınırlarının dar ve kesin çizgilerle çizilmesi elzemdir.

Karşı taraf buna rıza göstermiyorsa,[408] hedef sistemlere ağ üzerinden erişebilmek için bu sistemleri ağ üzerinden hacklemek ya da gizlice bu sistemlere malware enjekte etmek gerekir. Pratikte uzaktan aramanın bilfiil tatbik edilebilmesini sağlayan Alman Ceza Muhakemesi Kanunu(*StPO*) md. 100/b'de yer alan uzaktan arama düzenlemelerine dayanılarak işte tam da bu durumlar gerçekleştirilebilmekte ve arama yapabilmek için ağ/internet üzerinden sistemlere erişilebilmesi amacıyla sistemler hacklenebilmektetir. Sistemler hacklendikten sonra direkt olarak arama yapılabileceği gibi ağ üzerinden sistemlere rootkit ve spyware özelliklerine sahip malware yazılımlar yüklenerek, oluşturulan arka kapılar üzerinden de sistemler geniş bir zaman diliminde aranabilir. Yine gizli soruşturmacı kullanılarak sistemlere bir şekilde fiziki yollarla malware enjeksiyonu ve bilahare ağ üzerinden bu sistemlere erişilerek uzaktan aramanın tatbiki de gündeme gelebilir. CMK md. 134'ün lafzında ise uzaktan aramanın mümkün olabileceğine dair düzenlemeler yoktur. Bu haliyle eğer mevcut düzende CMK md. 134'ün uzaktan arama yöntemleriyle tatbikine girişilir ve sistemlere yetkisiz olarak ağ üzerinden erişilir ise bu durum TCK md. 243 gereğince yetkisiz erişim suçunu oluşturacaktır.

Doktrinde uzaktan aramanın yurt dışındaki mevcut uygulamaları eleştirilmekle birlikte,[409] Türk hukukunda da bu yönde bir düzenleme yapılması gerektiğine dair görüşler mevcuttur.[410] Kanaatimizce eğer imaj alma, imaj üzerinde inceleme ve en önemlisi de imajın bir örneğinin şüpheli/vekile verilmesine dair sorunlar aşılabilirse; Alman hukukundaki gibi son derece dar kapsamlı katalog suçlara yönelik, hackingin her aşamasının video kaydına alındığı ve yapılan tüm işlemlerin loglarının tutulduğu uygulamalar gündeme gelebilir. Fakat uzaktan aramada imaj alınamaz ve canlı sistemler üzerinde arama yapılmaya çalışılır ise hem deliller zarar görebilecek hem de fail/ortağı bu durumu fark ettiğinde, yanında kolluk olmadığı için sistemi alarak veya delilleri yok ederek kaçacaktır.

---

[408] ASS md. 32'de uzaktan aramaya dair failin/şüphelinin/veri sahibinin rızası aranmakta olup, etkili bir yöntem olmayan bu husus uzaktan arama noktasında zikredilmeyecektir.

[409] Muharrem ÖZEN ve Gürkan ÖZOCAK (2015), ''Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)'', *Ankara Barosu Dergisi*, S. 1, ss. 43-77, s. 51.

[410] Dijital Ceza Muhakemesi Hukuku, s. 475, 476.

Failler bilişim teknolojilerinden biraz anlıyorsa, suçlara konu verileri barındıran sistemlerin internet erişimine açık ağlarda yer almayacağını söylemek gerçekçi bir tahmin olacaktır. Bu sebeple çoğu zaman uzaktan aramanın sonucunda suça konu verilere erişilememesi ve fakat arama kararının icrası sırasında sistemdeki tüm özel verilerin(*bilgi*) gizliliğinin ihlali söz konusu olabilir. Ayrıca unutmamak gerekir ki bugün için USB içerisinde çalıştırılabilen işletim sistemleri mevcut olup, Tails gibi örnekler içerisinde ise azami anonimliği sağlayan gömülü yazılımlar bulunur. Bir hackerın cebinde taşıyarak herhangi bir cihazın portuna takıp çalıştırabileceği bu gibi sistem yazılımları içerisindeki suça konu verilerin de online arama yöntemiyle aranması pek mümkün değildir. Bu sebeple online arama yöntemleri, kanaatimizce elzem konular olarak görülmemeli ve temel haklar açısından her daim sakıncalı görülmelidirler.

3.3.1.2.2. Veri Trafiğinin İzlenmesi Amacıyla Sisteme Yetkisiz Erişimin Olanaklılığı Sorunu

Mevzuatımızda elektronik haberleşmenin dinlenilmesine/izlenmesine imkan tanıyan normlar bulunmaktadır. Bunlar; CMK md. 135, 2559 s. Polis Vazife ve Selahiyet Kanunu[411] ek md. 7, 2937 s. Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu[412](*MİT Kanunu*) md. 6 ve 2803 s. Jandarma Teşkilat, Görev ve Yetkileri Kanunu[413] ek md. 5'tir. Doktrinde genel olarak CMK md. 135'in internet iletişimine de tatbik edilebileceği belirtilmektedir.[414] Kanaatimizce de teoride bu normların her türlü elektronik haberleşme teknolojisi yönünden tatbiki mümkündür.[415]

Eğer gerekli kapasiteye sahip paket analiz teknolojileri(*DPI vb.*) kurulur ise tıpkı cep telefonunun dinlenmesi gibi elektronik haberleşme altyapısını kontrol eden erişim sağlayıcı işletmeciler üzerinden internet iletişimindeki çoğu husus dinlenebilir,

---

[411] Yayımlandığı R. Gazete: Tarih: 14/7/1934 Sayı: 2751
[412] Yayımlandığı R.Gazete: Tarih: 3/11/1983 Sayı: 18210
[413] Yayımlandığı R. Gazete: Tarih: 12/3/1983 Sayı: 17985
[414] Mustafa TAŞKIN (2011), *Adli ve İstihbari Amaçlı İletişimin Denetlenmesi*, Seçkin, Ankara, s. 83, 84, 85, 90, 200 vd.; Yasin SÖYLER (2013), *Kamu Hukuku Açısından İnternet İçeriğinin Düzenlenmesi ve Bu Alanda Devletin İdari Yaptırım Uygulama Yetkisi*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi, Ankara, s. 145; Cumhur ŞAHİN (2019), *Ceza Muhakemesi Hukuku Cilt 1*, Seçkin, Ankara, s. 355; Hakan KARAKEHYA (2016), *Ceza Muhakemesi Hukuku,* Savaş, Ankara, s. 355; Murat BALCI, M.Emin ALŞAHİN ve Kerim ÇAKIR (2021), *Ceza Muhakemesi Hukuku,* Adalet, s. 500; Dijital Ceza Muhakemesi Hukuku, s. 513.
[415] Sistem üzerinden gerçekleştiriliyor olsa bile iletişime dair verilere yönelik CMK md. 134 değil, 135. maddenin tatbiki gerekir. Aynı yönde bkz. Resul GÖKSOY (2019), *Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması,* Seçkin, Ankara, s. 175.

izlenebilir, gözlenebilir. Daha dar kapsamlı paket analiz teknolojileri ise trafiğe dair genel bilgilere ulaşılabilmesini sağlayacaktır. Şüphesiz ki erişim sağlayıcı işletmecilerin yardımı olmaksızın da erişime izin verilmiş bir yerel ağ üzerinden gerçekleşen iletişim izlenebilir. Yerel ağa bağlanılamıyor veya erişim sağlayıcı işletmeler üzerinden de trafik dinlenemiyor/izlenemiyor ise bu durumda ilk etapta istemci ile sunucudan birine sızılması ve trafiğin bu noktalardan izlenmesi gerekir. Bu durumda istemci veya sunucudan biri eğer erişime izin verir ise hukukilik açısından sorun yoktur. Lakin iki taraftan biri buna izin vermediğinde, sisteme erişim cebren ve hacking yöntemleriyle gerçekleştirilmek zorundadır. Trafiğin mitm konumunda izlenmesi için de proxy sunucular gibi aradaki bir sisteme erişilmesi gerekir. Bu durumda da eğer bu aradaki sistemin yetkilisi bu erişime izin vermiyorsa, sisteme cebren erişilmesi ve hacklenmesi gündeme gelecektir.

CMK md. 135 ve sair bir kanun hükmünü icra için ağ üzerinden bir sistem hacklendiğinde veya gizli soruşturmacı kullanımı ya da sair yöntemler ile fark ettirilmeden sistemlere fiziki yollarla malware enjekte edildiğinde, ‘’*elektronik haberleşmenin dinlenmesine/izlenmesine imkan tanıyan normların tatbiki için bilişim sistemlerine cebren erişilebileceği kabul edilmeyecekse*‘’, bu tür bir uygulama yetkisiz erişim suçunu oluşturacaktır. Kanaatimizce de böyle bir uygulamanın hukuka uygun olması mümkün değildir. Zira bir arama kararı olmaksızın soruşturma/kovuşturmalarda bilişim sistemlerine rızaya aykırı olarak erişilemez, arama kararları da dinleme/izleme kararlarının gerçekleştirilmesi için sistemlerin hacklenmesine yönelik değil, sistemlerde ‘’yüklü olan‘’ veriler vasıtasıyla delillerin elde edilebilmesine yönelik verilebilir. Kaldı ki temel hak ve hürriyetleri kısıtlayan normların açıkça düzenlenmiş olmaları gerekir ve mevzuatta bu yönde açık bir kanun hükmü de bulunmamaktadır.[416] Ayrıca tezin ilgili bölümlerinde zikredildiği üzere bu amaçla sistemlere sızdırılan Pegasus spyware; NATO raporlarına menfi olarak yansımış, hiçbir hükümet ve hukuk sistemi tarafından kullanıldığı kabul edilmemiş ve çoğu ülke tarafından kınanarak, kullanımı hukukun ötesinde de gayri meşru bir vaziyet almıştır. Resmi olarak Türkiye dahil hiçbir hukuk devletinin meşru kabul etmediği ve

[416] Bu noktada belirtmek gerekir ki dinlemeye/izlemeye imkan sağlayacak şekilde bilişim sistemlerine cebren erişim, sistem üzerinde belirli hakimiyet alanları yaratacak ve bu durum, sınırlı bir süre için salt belirli kanallardan yapılan iletişime yönelik verilen dinleme/izleme kararının kapsamını aşarak, sistemdeki sair pek çok uygulama üzerinden gerçekleşen trafiğin ve bunun ötesinde sistemde yüklü verilerin dokunulmazlığını da ihlal etmiş olacaktır. Yine bu dinlemelerin genellikle sisteme malware enjeksiyonu sonucu yapılabileceği göz önünde bulundurulur ise dinleme/izleme kararının süresi dolduktan sonra bu yazılımın sistemden nasıl kaldırılacağı da meçhuldür.

normatif altyapısı da bulunmayan bir sistemin, hukukun tatbiki için kullanımı ise pekala mümkün olamaz.

3.3.1.2.3. MİT Kanunu'nda Yer Alan Genel Erişim Yetkisi

MİT Kanunu md. 6'da MİT'in kanunda yer alan görevlerini yerine getirmeye yönelik kullanabileceği yetkiler arasında, bir kısım bilişim sistemlerine genel bir erişim yetkisi de bulunmaktadır. İlgili normda,

> ''*Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar*''

denilmekle, bu normun kapsamı içerisinde kalan bilişim sistemlerine MİT'in erişimi mümkün kılınmıştır.

3.3.1.2.4. Soruşturma Aşamasında Veri Tabanlarında Genel Tarama Yapılması

Alman hukukunda yer alan ve Rasterfahndung olarak adlandırılan, soruşturmalarda delillere ulaşabilmek adına araştırılacak alanların daraltılmasına yönelik veri tabanlarına erişilmesi ve bu veri tabanlarında ulaşılması amaçlanan delillere dair taramalar yapılmasının[417] Türk hukukunda meşruluğu tartışmalıdır. Doktrinde kamu veri tabanlarında bu tür bir genel erişim ve genel tarama yetkisinin CMK'nın mevcut yapısına göre mümkün olmadığını belirten görüşler mevcut olmakla birlikte,[418] bu yöndeki bir kısım yazar kanuna bu yönde bir düzenlemenin eklenmesinin suçla mücadelede faydalı olacağını belirtmektedir.[419]

Örneğin kolundaki ejderha dövmesinin kamera kayıtlarında görüldüğü ve yüzünün maskeli olduğu için seçilemediği bir failin tespiti için tek tek dövmeciler ile görüşülmesi zor olacaktır. Dövmecilerin veri tabanları ve surface web ile deep web içerikleri veri madenciliği-analizi yöntemleri ile taranır ise çok daha kolay biçimde

[417] Cengiz TANRIKULU 2014, age. s. 270, 271.
[418] Çiler Damla BAYRAKTAR (2018), ''Ceza Muhakemesi Hukukunda Bir Koruma Tedbiri Olarak Otomatik Veri Taraması (Rasterfahndung): İnsan Hakları Bağlamında Bir Analiz'', *Ceza Hukuku Dergisi*, C. 13, S. 38, ss. 25-64, s. 42, 43, 44, 53, 54, 55 vd.
[419] Cengiz TANRIKULU 2014, age. s. 277, 280.

failin tespiti mümkündür. Lakin şüphesiz ki yetkisiz kişilerin erişimine kapalı veri tabanlarına arama kararı olmaksızın erişilemeyeceği için bunlara genel erişim sağlayan bir sistem kurularak yapılan taramalar, teknik zorlukların yanında hukuken de mümkün değildir. Bu tür taramaların kamunun erişimine açık veri tabanlarında ve surface web ile deep web'in herkesin ulaşabileceği noktalarında yapılmasında ise herhangi bir sorun oluşmaz. Örneğin tipik bir veri madenciliği yazılımı ile internetin kamunun erişimine açık noktalarında dövme resminin taranması mümkündür. Zira herkesin erişebileceği alanlara savcılığın erişemeyeceğini ya da bunun için özel bir hakimlik kararının aranacağını söylemek mümkün değildir.

İkinci olarak kamu tüzel kişilerinin kontrolü altındaki veri tabanlarından, TCK md. 161 gereğince müzekkere ile bilgi talebi mümkün olduğundan ve bilgi vermekten kaçınılamayacağından, ilgili birimlerin kendi veri tabanlarında tarama yapması da pekala mümkündür. Lakin CMK md. 161'de ''*Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adlî kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir …*'' denilmiş olsa da mevcut düzende CMK'da bu yönde bir düzenleme olmadığından, soruşturma kapsamında bir yazılım geliştirilerek kamu veri tabanlarında spesifik taramalar yapılması söz konusu olamaz. Lakin TCK md. 243/1 noktasında tartışılması gereken konu, böyle bir durumda bu yönde bir karar alan savcı ve/veya yardımcı olan adli kolluk görevlilerinin taramayı gerçekleştirmesi durumunda kamu veri tabanlarına yetkisiz erişimlerinin yetkisiz erişim suçunu oluşturup oluşturmayacağıdır.

Savcılığın Adalet Bakanlığı bünyesinde tutulan veri tabanlarına, PTT kayıtlarına, İç İşleri Bakanlığı bünyesinde tutulan Polnet, KIHBİ ve trafik sicil kayıtları gibi sair veri tabanlarına, TAKBİS veri tabanına, Sağlık Bakanlığı ve SGK bünyesindeki bazı veri tabanlarına soruşturma kapsamında erişim yetkisi zaten mevcuttur.[420] Böyle bir durumda soruşturmalar kapsamında savcılığın UYAP ve sair sistem üzerinden direkt olarak erişebildiği bu gibi veri tabanları yönünden, UYAP kullanılmayıp farklı yazılımlar ile genel tarama gerçekleştirilmesi kanaatimizce hukuka uygun olacaktır. Lakin salt müzekkere ile talep edilebilen bilgiler konusunda veya bunların ötesinde MİT ya da TSK'nın devlet sırrı sayılabilecek veri tabanlarında tarama yapılamayacağı, bunlara direkt olarak erişimin TCK md. 243'te düzenlenen yetkisiz erişim suçunu oluşturacağı açıktır.

[420] https://uyap.gov.tr/Genel-Bilgi, (ET:02.03.2022).

3.3.1.2.5. Denetim Faaliyetleri

Mevzuatımızda yer alan bir çok normda düzenleyici ve denetleyici kurumların, denetim kapsamlarına giren işlere yönelik belirli bilgilere erişebileceği ve ilgililerin bu bilgilerin verilmesinden yahut yapılacak incelemelerden kaçınamayacağı, gerekiyorsa bunun cebren yapılacağı düzenlenmiştir. Bu düzenlemeler arasında bilişim sistemlerine erişim yetkisi verenler de bulunmaktadır.

Evvela BTK'nın denetim yetkisine dair Elektronik Haberleşme Kanunu'nda düzenlemeler mevcuttur. Elektronik Haberleşme Kanunu md. 59'da

> ''*... Kurum, bu Kanunun kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, mahallinde de inceleme ve denetim yapabilir ve/veya yaptırabilir. Mülki amirler, kolluk kuvvetleri ve diğer kamu kurumlarının amir ve memurları inceleme veya denetimle görevlendirilenlere her türlü kolaylığı göstermek ve yardımda bulunmakla yükümlüdürler. ... Denetimle görevlendirilenler, denetime tabi olanlar veya tesisleri nezdinde, defterler de dahil olmak üzere her türlü evrak ve emtianın, elektronik ortamdaki bilgilerin, elektronik haberleşme alt yapısının, cihaz, sistem, yazılım ve donanımlarının incelenmesi, suret veya numune alınması, konuyla ilgili yazılı veya sözlü açıklama istenmesi, gerekli tutanakların düzenlenmesi, tesislerin ve işletiminin incelenmesi konularında yetkilidir. Denetime tabi tutulanlar, denetimle görevli kişilere her türlü kolaylığı göstermek, yukarıda sayılan hususlarla ilgili taleplerini belirlenen süre içinde yerine getirmek, cihaz, sistem, yazılım ve donanımları denetlemeye açık tutmak, denetim için gerekli alt yapıyı temin etmek ve çalışır vaziyette tutmak için gerekli önlemleri almak zorundadır. Aykırı davranışta bulunanlara bu Kanun ve ilgili mevzuat hükümlerine göre cezai işlem uygulanır.*'' denilmiş, aynı kanun md. 60/12'de ise ''*Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkrada belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. ... Gerçek kişiler ile özel hukuk tüzel kişileri, Kurumun bu maddedeki görevleri ile ilgili taleplerini, tabi oldukları mevzuat hükümlerini gerekçe göstermek suretiyle yerine getirmekten kaçınamazlar.*''
>
> şeklinde bir düzenlemeye gidilmiştir.

İkinci olarak MASAK'ın bu yöndeki yetkisi, 5549 s. Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'da[421] düzenlenmiştir. İlgili kanunun 7. maddesinde

> ''*… kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlar, Başkanlık ve denetim elemanları tarafından istenilecek her türlü bilgi, belge ve bunlara ilişkin her türlü ortamdaki kayıtları, bu kayıtlara erişimi sağlamak veya okunabilir hale getirmek için gerekli tüm bilgi ve şifreleri tam ve doğru olarak vermek ve gerekli kolaylığı sağlamakla yükümlüdür. (2) Yukarıdaki fıkraya göre talepte bulunulanlar savunma hakkına ilişkin hükümler saklı kalmak kaydıyla, özel kanunlarda yazılı hükümleri ileri sürerek bilgi ve belge vermekten kaçınamazlar. ''* denilmiştir. Yine aynı kanunun 9. maddesinde, '' *(1) Kanunları veya faaliyet konuları gereğince, ekonomik olaylara, servet unsurlarına, vergi mükellefiyetlerine, nüfus bilgilerine ve yasa dışı faaliyetlere ilişkin kayıt tutan kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki kurum ve kuruluşların bilgi işlem sistemlerine Bakanlık ve ilgili Bakanlığın veya kamu kurumu niteliğindeki kurum ve kuruluşların yetkili organlarının birlikte belirleyeceği usûl ve esaslar dahilinde Başkanlıkça erişim sistemi kurulabilir. (2) Türkiye Cumhuriyet Merkez Bankası hariç kamu sermayeli bankalar ile kamu iktisadî teşebbüsleri birinci fıkra kapsamı dışındadır* ''

denilerek, ön alan araştırmasına yakın daimi bir denetim sistemi kurulabileceği zikredilmiştir.

Üçüncü olarak SPK'nın bu yöndeki yetkisi, 6362 s. Sermaye Piyasası Kanunu[422] md. 88 ve 89'da düzenlenmiştir. Madde 89'un ilgili kısmı şöyledir:

> ''*(1) Denetim, bu Kanun kapsamındaki tüm kurum ve kuruluş ile ilgili diğer gerçek ve tüzel kişilerin bu Kanun ve ilgili diğer mevzuatın sermaye piyasasına ilişkin hükümleriyle ilgili faaliyet ve işlemlerini kapsar. Denetimle görevlendirilen personel, ilgili gerçek ve tüzel kişilerden bu Kanun ve ilgili diğer mevzuatın sermaye piyasasına ilişkin hükümleriyle ilgili görecekleri bilgi ve belgeleri istemeye, bunların vergi ile ilgili kayıtları dâhil olmak üzere tüm defter ve belgeleri ile elektronik ortamda tutulanlar dâhil tüm kayıtlar ve sair bilgi ihtiva eden vasıtaları, bilgi sistemlerini incelemeye, bunlara erişimin sağlanmasını istemeye ve bunların örneklerini almaya, işlem ve hesaplarını denetlemeye, ilgililerden yazılı ve sözlü bilgi almaya, gerekli tutanakları düzenlemeye yetkilidir. (3) Kurul Başkanının talepte bulunması ve sulh ceza hâkiminin kararı üzerine gerekli yerlerde kolluk yardımı ile arama yapılabilir. Aramada bulunan ve incelenmesine lüzum görülen defterler ve belgeler ayrıntılı bir*

[421] Yayımlandığı Resmî Gazete: Tarih: 18/10/2006 Sayı: 26323
[422] Yayımlandığı Resmî Gazete: Tarih: 30/12/2012 Sayı: 28513

tutanakla tespit olunur ve yerinde incelemenin mümkün olmadığı hâllerde, muhafaza altına alınarak inceleme yapanın çalıştığı yere sevk edilir‘’.

3.3.1.2.6. Yer Sağlayıcının Başkasının Yetkisine Tahsis Ettiği Alandaki Verilere Müdahalesi

Yer sağlayıcıların, hosting hizmeti satın alan internet sitesi/uygulaması işletmecisi ile arasındaki anlaşmaya riayet etmesi ve keyfi olarak müşterisine tahsisli siber uzaya erişmemesi gerekir. Aynı şekilde bir internet sitesi işletmecisi de belirli bir bedel karşılığında üyelik hesapları satabilir ve sosyal medya örneklerinde olduğu gibi kişiler bu hesapları üzerinden haberleşmenin gizliliği dahilinde mesajlaşabilirler. İnternet sitesi işletmecisi de bu mesajları keyfi olarak okuyamaz yahut bu tür verilere müdahale edemez.

Pratikte yer sağlayıcıların ve/veya internet sitesi/uygulaması işletmecilerinin başkalarına tahsisli bu tür alanlara yani özünde ‘’bilişim sistemlerine‘’ erişebilmesi, karşı taraf ile yaptıkları sözleşmelerde yer alan kayıtlardan dolayı mümkün olmaktadır. Bu tür kayıtlar ise hakkın kullanılması hukuka uygunluk sebebi ile ilgili olup, bu alt başlığın konusu değildir. Kanun hükmünü icra noktasında değerlendirilmesi gereken husus, mevzuatta yer sağlayıcılara yönelik getirilmiş bağlayıcı düzenlemeler bulunmasıdır. Yer sağlayıcıların bu düzenlemelerin gereği olarak başkalarına tahsisli alanlara erişmesi ve veriyi internet trafiğine yönelik bloklaması yahut doğrudan silmesi gerekmektedir.

5651 s. Kanun md. 5/2’de yer alan ‘’*Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde yayından çıkarmakla yükümlüdür.*‘’ şeklindeki düzenlemeden kaynaklanan bu durum, ortada bağlayıcı bir idari karar yahut mahkeme kararı mevcut ise yer sağlayıcı bakımından direkt olarak hukuka uygunluk sebebi sayılacaktır. Fakat uyar-kaldır başvuruları noktasında bu yönde kesin bir kanaate varmak mümkün olmayıp, yanlış uyarılar sonucu işlem gerçekleştirilmesi TCK md. 243 ve 244’teki suçları oluşturabilir.[423]

[423] Uyarılar sonucu içeriğin kaldırılması noktasında yer sağlayıcıların durumu yönünden ayrıntılı bilgi için bkz. Alp ÖZTEKİN 2021, age. s. 218, 219.

3.3.1.2.7. Hüküm Sonucunun Tatbiki İçin Bilişim Sistemlerine Erişim Gerektiren İlamların İcrası

Hukuk mahkemesi kararında yer alan hüküm sonucunun tatbiki için bir bilişim sistemine erişilmesi gereken durumlarda, davacı bu sonucu yaratmak için kendiliğinden hareket edemez. Normal şartlar altında İİK md. 30 gereğince bu tür ilamlar icraya konulur ve karşı tarafa bunu yapması emredilir. Örneğin bir borçlu online oyun karakteri içerisindeki eşyaları ya da üçüncü taraf sunucularda barındırılan kripto varlıklarını(*örn. NFT koleksiyonu*) alacaklıya aktaracağına dair belirli bir bedel karşılığı sözleşme yapmış olabilir. Borçlu daha sonra bu borçlarını ifa etmemiş ve buna yönelik açılan davayı da kaybetmiş ise hüküm sonucu İİK'ya göre icraya konularak borcun ifası emredilecektir. Olağan durumlarda ilgilisi işi yapmadığında, iş cebren yaptırılır. Lakin eldeki durumda böyle bir sonuca ulaşmak için borçlunun üyelik hesabının ya da üçüncü taraf şirketlerin sistemlerinin hacklenmesi gerekecektir. Böyle bir uygulama ise İİK'nın mevcut yapısı ile bağdaşmamaktadır. Bu sebeple bilişim sistemlerine cebren erişimi kapsayan durumların salt takip borçlusunun yapabileceği işler sayılması gerekir ve eğer bu yönde bir ilam icraya konulduktan sonra takibin gereği olarak sisteme yetkisiz olarak erişilir ise İİK md. 30 bir hukuka uygunluk sebebi oluşturmayacaktır.[424]

3.3.1.3. Meşru Savunma

TCK md. 25/1'de düzenlenen meşru savunma; gerçekleşme ihtimali kuvvetle muhtemel yahut gerçekleşmekte olan bir haksız saldırının defedilmesi için savunma yapılma zorunluluğu doğduğunda, saldırıya yönelik orantılı biçimde gerçekleştirilen ve saldırının/devamının önlenmesine yönelen eylemlerin gerçekleştirilmesi durumunda bulunur.[425] Doktrinde meşru savunmanın TCK md. 243'e yönelik bir hukuka uygunluk sebebi teşkil edebileceği yönünde görüşler mevcuttur.[426] Bir kısım

[424] Bu konuda detaylı açıklamalar için bkz. Alp ÖZTEKİN 2021, age. s. 606, 607, 608.
[425] Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2021, age. s. 219, 220; Fatih Selami MAHMUTOĞLU ve Serra KARADENİZ (2017), *Türk Ceza Kanunu Genel Hükümler Şerhi*, Beta, İstanbul, s. 505, 506; Doğan SOYASLAN 2020a, age. s. 390, 391.
[426] Ahmet GÜL 2021, s. 106, 107; Meral EKİCİ ŞAHİN ve Irmak KORUCULU 2019, s. 610, 611; Barış Emre ALP (2019), *Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu*, Adalet, Ankara, s. 103, 104; İrem GEÇMEZ (2020), *Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları,* Seçkin, Ankara, s. 97, 99; Zeki AVŞAR ve Gürsel ÖNGÖREN 2010, age. s. 138; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1159.

görüş ise meşru savunmanın bilişim suçları yönünden gündeme gelemeyeceği yönündedir.[427]

Bir bilişim sistemine yetkisiz olarak erişmek veya kalmaya devam etmek durumunun herhangi bir savunma amacıyla kullanılması pek olası olmasa da kanaatimizce imkansız da değildir. Savunmaya yönelik bir durum ancak hedef sistem hakkında bilgi edinmek ya da haksız saldırıyı teşkil eden durumu ortadan kaldırmak için sisteme önceden erişilmesi gerektiğinde gerçekleştirilebilir. Örneğin bir internet sitesinde kişinin müstehcen görüntüleri yayınlanıyor ise bu yayını kesmek ya da sunucuları tamamen bozmak için DoS/DDoS saldırıları yahut zararlı kodların gönderimi söz konusu olabilir. Ancak bu tür saldırılar sadece yayını bir süre keseceği gibi ağır saldırılar da direkt olarak sistemi bozacağından, meşru savunma yönünden bu tür yöntemler orantılı olmayabilir. Öyleyse yayına dair verileri silmeye yönelik orantılı bir meşru savunmada sunuculara bir şekilde erişilerek bu verilerin silinmesi gerekecektir.

Yukarıdaki örnekte meşru savunma TCK md. 244 yönünden gündeme gelecek olup, TCK md. 243/1 savunmadaki öncül hareketleri tipikliğinde barındıran bir suç konumunda bulunacaktır. Tezin içtima bölümünde detaylı olarak tartışıldığı üzere TCK md. 244'e konu fiilleri gerçekleştirmek için sisteme yetkisiz olarak erişilmiş ise bu durumda cezalandırmanın nasıl yapılacağı konusunda doktrinde fikir birliği yoktur. Eğer sisteme yetkisiz olarak erişilir ve haksız saldırıyı oluşturan veriler silinir ise ve böyle bir durumda TCK md. 244 yönünden meşru savunmanın silme fiilini hukuka uygun kılacağı yönünde bir görüş benimsenirse, failin TCK md. 243'ten cezalandırılması meşru savunmaya dair TCK md. 25'in ruhuna aykırı olacaktır. Öyleyse sunucudaki verilerin silinmesinin şart olması gibi durumlarda TCK md. 244'e konu fiili gerçekleştirmek için sisteme erişmek gerekiyor ise ve yapılan eylemler TCK md. 244 yönünden meşru savunma sayıldığı için hukuka uygun kabul ediliyorsa, bu durumun TCK md. 243 yönünden de fiili hukuka uygun kılacağının kabulü gerekir. Lakin kişinin olayın özelliği sebebiyle sisteme erişmeden de savunma yapması mümkün olabiliyor ise TCK md. 243 yönünden meşru savunmanın kabulü TCK md. 25'in ruhuna uygun olmayacaktır. Zira bu tür bir eylem, saldırı-savunma arasında açık bir orantısızlık yaratacaktır.

[427] Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2012, age. s. 444; Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 964; Murat Volkan DÜLGER 2022, age. s. 300, 301; Burak Cesur AKÖZ 2018, age. s. 93, 94; Ali KARAGÜLMEZ 2014, age. s. 75.

Bizce kınanabilirlik içerisinde değerlendirilmesi gereken bir mesele olan, ‘’*özel kişilerin başka türlü toplanamama ihtimali bulunan delilleri elde etmesi*‘’ durumu doktrin[428] ve yargı kararlarında[429] meşru savunma özelinde değerlendirilebildiğinden, TCK md. 243’ün ve bilişim sistemlerine yetkisiz erişimin delil elde etmeye yönelik fiiller boyutuyla da ele alınması mümkündür.

3.3.1.4. Rıza

TCK md. 26/2’de düzenlenen rızanın bir hukuka uygunluk sebebi olarak TCK md. 243 bağlamında uygulanması konusunda doktrinde herhangi bir tartışma bulunmamaktadır. Hatta bazı görüşlere göre bu suç ile bağdaşabilen tek hukuka uygunluk sebebi yetkili olma durumudur. İlgili görüşte bu yetkili olma durumu için sanıyoruz ki kanun hükmü ya da rıza sonucu elde edilen yetkiye işaret edilmektedir.[430] İçtihatlar noktasında da rıza, bu suç bakımından bir hukuka uygunluk sebebi olarak değerlendirilmektedir.[431]

Rızanın bir hukuka uygunluk sebebi olabilmesi için mağdur tarafından fiil gerçekleştirilmeden önce verilmesi gerekir. Bu sebeple sisteme yetkisiz olarak erişildikten sonra verilen bir rıza, suçun oluşumu etkilemeyecek[432] ve ancak geleceğe yönelik olarak bir hukuka uygunluk sebebi teşkil edebilecektir. Açık rıza konusundaki tipik ve en teknik örnek sızma testleridir. Önceden yapılan sözleşmeler sonucu kapsamının çizildiği erişim yetkisinin beyaz şapkalı hackerlara verildiği sızma testlerinde, şekil şartı aranmayan sözleşmeler rızaya dayalı bir hukuka uygunluk sebebi teşkil edecektir.[433]

---

[428] Ersan ŞEN (2008), *Telefon Dinleme, Gizli Soruşturmacı, X Muhbir*, Seçkin, Ankara, s. 138.
[429] Yargıtay CGK 2010/5-187 E. 2011/131 K.
[430] Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2012, age. s. 444 / Aynı yönde bkz. Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 964.
[431] Rıza ile sosyal medya hesabına girme örneği için bkz. ‘’*... Olay tarihinde Facebook hesabıma erişim sağlayamadım. Şifremin kırılarak girildiğini tespit ettim. Bununla ilgili olarak her ne kadar sanığın IP numarası üzerinden bağlantı yapıldığı tespit edilmiş ise de T.... benim nişanlımdır, yakında da evleneceğiz, bu eylemi T.....'ın gerçekleştirdiğini düşünmüyorum. Bunu yapması için bir neden yoktur, benim şifrelerim zaten T....'da vardı. Benim hesabıma bu şekilde her zaman girebilirdi. Onun IP numarasından bağlantı yapılması bu nedenle normaldir. Şikayetimden vazgeçiyorum." şek- lindeki ifadesi karşısında; sanığın, şikayetçinin rızası dışında giriş yaptığına ilişkin delil bulunmadığından, beraati yerine yetersiz gerekçeyle mahkumiyetine karar verilmesi ...*‘’ Yargıtay 8. CD 2015/7077 E. 2015/24705 K.
[432] Zeki HAFIZOĞULLARI ve Muharrem ÖZEN 2012, age. s. 444; Aksi yönde ve sisteme hukuka aykırı olarak erişildikten sonra verilen rızanın, suçun mütemadi suç özelliği gereğince geçmişe yönelik de hukuka uygunluk yaratacağına dair görüşler için bkz. Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 964.
[433] Ahu Karakurt EREN 2020, age. s. 752, 753; Murat Volkan DÜLGER 2022, age. s. 652, 653.

Bu alt başlıkta değerlendirilmesi gereken esas meseleler ise zımni rıza, varsayılan rıza ve kısmi rıza kavramlarıdır. Bir kişinin her daim önceden rızasını açıkça dile getirmesi gerekmez. Zımni rıza olarak adlandırılabilecek bu durumlarda da fiil hukuka uygun sayılacaktır. Bilişim sistemlerine erişim konusunda zımni rızanın gündeme gelebileceği bir çok durum meydana gelebilir. Örneğin bir aile içinde kardeşlerden biri diğerinin bilgisayarını açar ve diğeri de ses etmez ise zımni rızanın varlığından bahsedilebilecektir. Varsayılan rıza ise objektif olarak toplum tarafından kabul edilen ve meşru görülen konularda, rızanın hukuki yönden varsayılacağı durumlarda gündeme gelir.[434] Örneğin bir restoranda wi-fi ağına ‘’müşteriler bağlanamaz‘’ şeklinde bir uyarı yoksa ve SSID şifresiz olarak görülüyor, herkes de ağa bağlanabiliyor ise bu noktada restoranlardaki genel uygulamalar dolayısıyla müşterilerin bu sisteme erişimi noktasında varsayılan rızadan bahsedilecek ve erişim hukuka uygun olacaktır. Lakin aynı durum müşteri olmayanlar ve örneğin sokaktan geçenler ya da bedava internet kullanımı için ağa erişen sair kişiler için geçerli olmayacak, bunların fiilleri hukuka aykırılık teşkil edecektir.

Doktrinde bilişim sistemlerinde şifreleme yahut yetkisiz erişimlere karşı sair bir güvenlik önleminin alınmamış olması zımni rıza çerçevesinde değerlendirilmiş ve bu durumlarda zımni rızanın gündeme gelemeyeceği belirtilmiştir.[435] Şifre konulmaması gibi durumlarda şüphesiz ki her olayda rızanın varlığından bahsedilemeyecek ise de bu durumun bizce varsayılan rıza içerisinde değerlendirilmesi ve yukarıdaki örnekteki gibi her durumun kendi özelinde değerlendirilmesi gerekir. Örneğin bir Yargıtay kararına da yansıdığı üzere iki ortağın birbirinin sistemlerine erişim izni vermiş olacaklarına dair bir varsayılan rıza anlayışının kabulü mümkün olmayacak, bu yönde açık ya da zımni bir rıza aranacaktır.[436] Lakin anne, baba ve tek çocuktan oluşan bir ailede babanın kendisine

---

[434] Veli Özer ÖZBEK 2010, age. s. 460.

[435] Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1158; Uğur İHTİYAROĞLU 2020, a.g.e, s. 428.

[436] ‘’*... yapılan soruşturma sonunda, taraflar arasındaki iş ortaklığı nedeniyle şüphelinin müştekinin e-posta hesabının şifrelerinin bilmesinin hayatın olağan akışına uygun olduğu gerekçesiyle kovuşturmaya yer olmadığına dair karar verildiği anlaşılmış olup; her ne kadar şüpheli savunmasında iş ortaklığının sona erdiği 24/01/2019 tarihine kadar müştekiye ait internet sitesinin yetkilisi olduğunu ileri sürmüş ise de, bu hususa ilişkin herhangi bir delil ya da belge sunamadığından 5271 sayılı Ceza Muhakemesi Kanunu'nun 170/2. maddesi gereğince; "Soruşturma evresi sonunda toplanan deliller, suçun işlendiği hususunda yeterli şüphe oluşturuyorsa; Cumhuriyet savcısı, bir iddianame düzenler." hükmü gereğince, soruşturma evresi sonunda toplanan delillerin suçun işlendiği hususunda yeterli şüphe oluşturması sebebiyle kovuşturmaya yer olmadığına dair karara karşı yapılan itirazın kabulü yerine yazılı şekilde reddine karar verilmesi, ...*‘’ Yargıtay 8. Ceza Dairesi 2020/4126 E 2021/18481 K.

aldığı tableti zaman zaman anne ya da çocuğun kullanması söz konusu oluyor ve baba bu durumu açıkça yasaklamıyor ise babanın zımni rızası ve haberi dahi olmasa, bu yönde bir varsayılan rızadan bahsedilebilecektir.

Kısmi rıza verilmesi durumunda ise sisteme belirli sınırlar dahilinde erişilmesine rıza gösterilmiş olacağından, sınırların aşılması durumunda TCK md. 243'te düzenlenen yetkisiz erişim suçu oluşacaktır.[437] Sanallaştırma uygulamaları haricinde tek fiziki sistem içerisinde başka bir bilişim sistemine erişme durumu gerçekleşemeyeceğinden, kanaatimizce böyle bir durumda tek bir uygulama yazılımının kullanılmasına rıza gösterilmesine rağmen farklı işlemler yapılması gibi ihtimallerde, yetkili olarak erişilen sistemde ''yetkisiz olarak kalmaya devam etme'' seçimlik hareketi sebebiyle suç oluşacaktır. Lakin birden çok sanal birime ayrılmış bir bilişim sisteminde tek ara yüz yönünden erişimine rıza gösterilen kişi öteki ara yüze yetkisiz şekilde erişir ise suç, sisteme yetkisiz erişim seçimlik hareketi yönünden oluşacaktır.

Rızanın bir hukuka uygunluk sebebi sayıldığı durumlarda bilişim sistemlerine erişime dair bir kısım tartışmalı durumların yaşanması mümkündür. Özellikle phishing yöntemleri kullanılarak mağdurların o noktalara çekilmesi sonucu veya tesadüf eseri o bağlantıya tıklayan yahut indirme işlemlerini başlatan kişilerin sistemlerine malware enjekte edilmesi durumunda, hackerlar faillerini sübjektif özellikleri yönünden seçemezler. Failin phishing yöntemlerini kullanarak, oluşturduğu sahte ikiz web sitesi üzerinden ziyaretçileri belirli bağlantılara tıklatmaya ve bu sayede sistemlerine malware enjekte edilmesine sebep olduğu bir durumda, mağdurların failin yakın arkadaşı ya da kardeşi olması mümkündür. Örneğin böyle bir durumda failin zaten erişim yetkisinin bulunduğu veya varsayılan rıza noktasında var kabul edildiği yakın arkadaşının sistemini hacklemesi neticesi doğabilir. İlgili bölümde zikredildiği üzere malware çalıştırıldığı/otomatik olarak çalıştığı an erişim ve hakimiyet imkanı sunuyor ise sisteme erişim gerçekleşmiş sayılacaktır. İşte böyle bir durumda failin zaten rıza sebebiyle yetkisinin bulunduğu bir sistemi, yetkisinin olmadığı üçüncü bir sistemi hacklemek isterken hacklemesi mümkündür. Doktrinde bir kısım görüş, hukuka uyguluk sebeplerinin objektif olduğunu ve failin sübjektif hissiyatı ile kastının bu noktada önemli olmadığını, fail hukuka uygunluk durumunu bilmese dahi hukuka

[437] Büşra ÖZÇELİK 2019, age. s. 78.

uygunluk sebebinin tecelli edeceğini belirtmektedir.[438] Zıt yöndeki görüşler ise hukuka uygunluk sebeplerinin sübjektif olarak değerlendirileceğini ve fail hukuka uygunluk sebebinin oluşmadığını düşünerek suç işleme iradesiyle hareketi gerçekleştirmiş ise fiilin hukuka aykırı kabul edileceğini belirtmektedir.[439] TCK md. 243 yönünden haksızlık bilinci arandığından, failin haksızlık bilinci içerisinde ve hukuka uygunluk durumunu bilmeden gerçekleştirdiği bu tür hacking eylemleri yönünden suçun objektif ve sübjektif tipikliği oluşacaktır. Hukuka uygunluk sebeplerinin objektifliği kabul edildiğinde ise failin beraatine karar verilecektir.[440]

3.3.1.5. Hukuka Uygunluk Sebeplerinin Gerçekleştiği Konusunda Kaçınılmaz Hataya Düşülmesi

TCK md. 30/3'te ''*Ceza sorumluluğunu kaldıran veya azaltan nedenlere ait koşulların gerçekleştiği hususunda kaçınılmaz bir hataya düşen kişi, bu hatasından yararlanır*.'' denilmiştir. Kanun'da ceza sorumluluğunu kaldıran veya azaltan nedenler bölüm başlığı altındaki maddeler içerisinde hukuka uygunluk sebepleri ve kusurluluğu/kınanabilirliği kaldıran durumlar birlikte düzenlenmiştir. Bu sebeple TCK md. 30/3'ün bir yanı hukuka uygunluk sebepleri diğer yanı ise kusurluluğu kaldıran sebepler ile ilgilidir.[441]

Doktrin ve içtihatlardaki ağırlıklı görüş, hukuka uygunluk sebeplerinin gerçekleştiği konusunda kaçınılmaz bir hataya düşen faildeki kast ve/veya taksirin ortadan kalkacağı yönündedir.[442] Yetkisiz erişim suçunun sübjektif tipikliğinin oluşabilmesi için zaten kişinin eylemlerindeki hukuka aykırılığın bilincinde olması

---

[438] Bu yöndeki görüşler için bkz. Fatih Selami MAHMUTOĞLU ve Serra KARADENİZ 2017, age. s. 710; Doğan SOYASLAN 2020a, age. s. 362, 363; Nevzat TOROSLU ve Haluk TOROSLU 2021, age. s. 160; Timur DEMİRBAŞ 2021, age. s. 463.

[439] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE (2021b), *Türk Ceza Hukuku Genel Hükümler*, Onaltıncı Basım, Seçkin, Ankara, s. 282; Mahmut Koca ve İlhan Üzülmez (2021), *Türk Ceza Hukuku Genel Hükümler*, Ondördüncü Basım, Seçkin, Ankara, s. 271.

[440] Kanaatimizce hukuka uygunluk sebepleri failin sübjektif bilinci değil, objektif olarak maddi dünyada mevcut olan hukuka uygunluk vaziyeti ile ilgilidir. Bu sebeple failde haksızlık bilinci mevcut olsa dahi maddi dünyada mevcut olan objektif hukuka uygunluk gereğince suç oluşmayacaktır. Lakin failin meşru savunma imkanını bilmeden haksızlık bilinci içerisinde birini öldürmesi gibi bir durumda, fiilin hukuka uygunluğu failin katil olduğu gerçeğini ve toplum açısından tehlike yarattığını yani ıslahının gerektiği olgusunu değiştirmeyecektir. Öyleyse bu tür durumlarda faillerin güvenlik tedbirleri altında ıslahına çalışılmalı ve bu yönde TCK ile CMK'da değişikliğe gidilmelidir.

[441] Bahri ÖZTÜRK ve Mustafa Ruhan ERDEM 2021, age. s. 479

[442] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021b, age. s. 438, 439 vd.; Berrin AKBULUT 2018, age. s. 520, 521; İzzet ÖZGENÇ 2021, age. s. 527; Mahmut KOCA ve İlhan ÜZÜLMEZ 2021, age. s. 300, 301; Fatih Selami MAHMUTOĞLU ve Serra KARADENİZ 2017, age. s. 708, 709 / Bu durumda failin hukuka uygunluk sebebinden yararlanması gerektiği yönündeki görüşler için bkz. Bahri ÖZTÜRK ve Mustafa Ruhan ERDEM 2021, age. s. 481.

gerektiğinden, hukuka uygunluk sebeplerinin gerçekleştiği konusunda kaçınılmaz bir hataya düşen fail hakkında hem suçun unsurları içerisindeki haksızlık bilincinin yokluğu hem de TCK md. 30/3 devreye girecek, her iki norm da sübjektif tipikliğin oluşumunu engelleyecektir. Zira hukuka uygunluk sebepleri noktasında kaçınılmaz bir hataya düşen failde haksızlık bilinci bulunduğunu söylemek mümkün olamamaktadır.

3.4. SUÇUN KINANABİLİRLİK UNSURU (*Kusurluluk*)

CMK md. 223/3'e göre

''*yüklenen suçla bağlantılı olarak yaş küçüklüğü, akıl hastalığı veya sağır ve dilsizlik hali ya da geçici nedenlerin bulunması, yüklenen suçun hukuka aykırı fakat bağlayıcı emrin yerine getirilmesi suretiyle veya zorunluluk hali ya da cebir veya tehdit etkisiyle işlenmesi, meşru savunmada sınırın heyecan, korku ve telaş nedeniyle aşılması, kusurluluğu ortadan kaldıran hataya düşülmesi*''

durumlarında, sanığın kusurunun bulunmaması[443] sebebiyle ceza verilmesine yer olmadığına dair karar verilecektir. Benimsenen görüşler gereğince bu durumlar suçun kınanabilirlik/kusurluluk unsuru içerisinde değerlendirilirler.[444]

Yetkisiz erişim suçunda kınanabilirlik yönünden önem arz eden pek bir husus yoktur. Bu noktada değinilmesi gereken tek mesele kişilerin başka suretle elde edilemeyeceğini düşündükleri delilleri elde etme amacıyla bilişim sistemlerine yetkisiz olarak erişmeleridir. Hukuka uygunluk sebepleri açıklanırken zikredildiği üzere doktrin ve yargı kararlarında bu durum genel olarak hukuka uygunluk sebepleri içerisinde değerlendirilmekte, ayrıca sübjektif tipiklik açıklanırken aktarıldığı üzere bu yönde haksızlık bilinci yönünde yapılan sair değerlendirmeler de bulunmaktadır. Kanaatimizce ''bir daha delil elde edilememesi ihtimali'' açıkça bir zorunluluğa işaret ettiğinden, bu noktada bu tür eylemlere girişen fail yönünden şartları mevcut ise

[443] CMK md. 223/2-b'de kast ve taksirin bulunmaması durumu ayrıca düzenlenmiş ve bu durumda beraat kararı verileceği belirtilmiştir. CMK md. 223/3'te ise özellikle kusurluluk ve kusur kavramları kullanılmış, ikinci fıkrada kast ve taksir ayrıca düzenlendiği için kusurluluk, kast ve taksirden ayrıştırılmıştır. Kanun koyucu CMK md. 223/3'te kusurun bulunmaması halinde yani kusurluluğu kaldıran durumların varlığında beraat kararı verileceğini düzenlemese de ''suçun oluştuğuna'' dair bir duruma işaret etmemektedir. Yine maddenin ikinci fıkrasında da yalnızca bu durumlarda suçun oluşmamış kabul edileceğine dair bir vurgu yoktur. Bilakis CMK md. 223/4'te kanun koyucu ''işlenen fiilin suç olma özelliğini devam ettirmesine rağmen'' diyerek, iki ve üçüncü fıkralardaki durumların varlığında ortada tamamlanmış bir suçun olmadığını, dördüncü fıkradaki etkin pişmanlık ve sayılan sair hususların varlığında ise artık tüm unsurları ile oluşan fakat cezalandırılmayacak bir suçun söz konusu olduğunu açıkça vurgulamaktadır. Öyleyse CMK'nın ruhuna göre suçun unsurları objektif-sübjektif tipiklik, hukuka aykırılık ve kınanabilirlik/kusurluluk olmalıdır.

[444] Bu konuda bkz. Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021b, age. s. 209, 358, 359 / Bahri ÖZTÜRK ve Mustafa Ruhan ERDEM (2008), *Uygulamalı Ceza Muhakemesi Hukuku*, Seçkin, Ankara, s. 165, 282, 283 vd.

zorunluluk halinin mevcudiyeti[445] sebebiyle suçun kınanabilirlik unsuru oluşmayacaktır.

Kınanabilirlik alt başlığı altında değerlendirilmesi gereken bir diğer konu ise suçun kınanabilirlik unsurunu kaldıran, haksızlık bilincine yönelik bir hataya düşülmesi halidir. TCK md. 30/4'te kişinin eyleminin *haksızlık teşkil edip etmediği konusunda kaçınılmaz bir hataya düşmesi* halinde hatasından yararlanacağı düzenlenmiştir. Failin fiilinin haksızlık teşkil etmediğini düşünmesi ve bu durumun fail yönünden kaçınılmaz bir hata olarak kabul edilebilmesi halinde, katıldığımız görüşlere göre bu durum kınanabilirliği kaldıracaktır.[446] Doktrinde spesifik olarak TCK md. 243 bağlamında yapılan değerlendirmelerde de haksızlık bilinci konusundaki kaçınılmaz hatanın, kınanabilirliği kaldıracağı belirtilmektedir.[447] Lakin yetkisiz erişim suçu yönünden hareketin zaten haksızlık bilinci içerisinde gerçekleştirilmesi gerektiğinden ve bu durumda hata kaçınılabilir olsa dahi suçun sübjektif tipikliği oluşmayacağından, kanaatimizce TCK md. 30/4 bu noktada devreye giremez.

3.5. SUÇUN NETİCESİ SEBEBİYLE AĞIRLAŞMIŞ HALİ

3.5.1. Genel Olarak

TCK md. 243/3'te normun birinci fıkrasındaki seçimlik hareketler kastedilerek, ''*Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur*'' denilmiş ve bu suretle yetkisiz erişim suçu yönünden gerçek[448] bir neticesi sebebiyle ağırlaşmış suç tipi yaratılmıştır. Doktrindeki görüşler[449] de bu yönde olduğu gibi maddenin gerekçesinde[450] de bu husus açıkça zikredilmiştir.

---

[445] Hamide ZAFER (2010), *Özel Hayatın Gizli Alanının Ceza Hukukuyla Korunması*, Beta, İstanbul, s. 111.

[446] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021b, age. s. 445; Mahmut KOCA ve İlhan ÜZÜLMEZ 2021, age. s. 370; Bahri ÖZTÜRK ve Mustafa Ruhan ERDEM 2021, age. s. 480; Yargıtay. 16. CD 2019/3288, E. 2019/1284 K.

[447] Cengiz APAYDIN 2017, age. s. 73.

[448] Kast-taksir kombinasyonu bulunan neticesi ağırlaşmış suç tiplerine gerçek neticesi sebebiyle ağırlaşmış suçlar denilir. Bu konuda bkz. Mahmut KOCA ve İlhan ÜZÜLMEZ 2021, age. s. 247; Fatih Selami MAHMUTOĞLU ve Serra KARADENİZ 2017, age. s. 401.

[449] Berrin AKBULUT 2017, age. s. 112; Ali İhsan ERDAĞ 2010, age. s. 282; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 904; Ali KARAGÜLMEZ 2014, age. s. 212; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 241; Doğan SOYASLAN 2020b, age. s. 666; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1154.

[450] Madde gerekçesi: *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*

Aşağıda neticesi sebebiyle ağırlaşmış bir suç tipi olan TCK md. 243/3 ile yetkisiz erişim suçunun temel halinin unsurları yönünden farklılaşan bir kısım önemli hususlar aktarılmış, bu yönde neticesi sebebiyle ağırlaşmış suçun tipiklik ve hukuka aykırılık unsurları incelenmiştir. Kınanabilirlik unsuru yönünden önem arz eden bir durum bulunmadığı için suçun bu unsuru ayrıca incelenmemiştir.

3.5.2. Suçun Tipiklik ve Hukuka Aykırılık Unsurlarının Neticesi Sebebiyle Ağırlaşmış Hal Nazarında Değerlendirilmesi

3.5.2.1. Objektif Tipiklik Yönünden Değerlendirme

TCK md. 243/3'te düzenlenen neticesi sebebiyle ağırlaşmış suç tipinin objektif tipikliğinin oluşabilmesi için hareketin tekliği gerekir. Gerçekleşmesi gereken hareket ise TCK md. 243/1'deki seçimlik hareketler olan girme/erişme ve kalmaya devam etmedir. Kastedilen neticenin ve bundan ayrı olarak bilahare ağırlaşan bir neticenin meydana geldiği neticesi sebebiyle ağırlaşmış suçlarda iki ayrı netice gerçekleşir. Örneğin bir kişi önce hafifçe yaralanır ve bu netice gerçekleşir, bilahare kişi pıhtılaşma sorunu nedeniyle ölür ise ölüm neticesi de gerçekleşecek ve neticesi sebebiyle ağırlaşmış bir yaralama suçu meydana gelecektir. TCK md. 243/3'te ''*Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse*'' denildiğinden, sisteme erişme/kalma neticesinden ayrı olarak, hareketlerin ayrıca verilerin yok olmasına ya da değişmesine de sebep olması gerekir.

Bilişim sistemine erişim, sistemin başında öylece oturmak ya da ağ bağlantısını sağladıktan sonra hiçbir hareket gerçekleştirmemek ile sınırlı bir eylem yapısı olmadığından, sistemde çeşitli işlemler gerçekleştirilmesi ve örneğin farklı uygulama yazılımlarının çalıştırılması veya dosyaların açılması eylemleri de TCK md. 243/1'in objektif tipikliği içerisinde değerlendirilir. Öyleyse örneğin fail sisteme eriştikten sonra şifreli bir veri dosyasını açmaya çalışır ve eğer şifrelemeyi sağlayan yazılım bulutta arşivli olan verileri saldırı anında silmek üzerine programlanmışsa, fail istemeden de olsa verilerin silinmesine sebep olacaktır. Bu durumda ne yetkisiz erişim suçunun temel hali olan TCK md. 243/1 ne de bilişim sistemlerindeki verileri yok etmeyi ya da değiştirmeyi suç olarak düzenleyen temel norm olan TCK md. 244/2 değil, yetkisiz erişim suçunun ''verilerin yok olması neticesi sebebiyle'' ağırlaşmış hali olan TCK md. 243/3 oluşacaktır. Yukarıda malware tipi yazılımlar ve bunların

öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.

çeşitli özellikleri aktarılırken belirtildiği üzere, bunlardan bir kısmı verileri silme ve değiştirme özelliğine sahiptir.[451] Faile sisteme erişim ve hakimiyet yetkisi kazandıran bir malware, siber güvenlik yazılımı tarafından yapılan taramalar sırasında keşfedildiği ve yok edileceğini anladığı sırada eğer verilere zarar vermiş ve failin bu netice yönünden taksiri mevcutsa bu durumda da TCK md. 243/3 uygulama alanı bulabilir.

Eğer fail sisteme erişimi sürerken TCK md. 243/1'in tipikliği dışında kalan ikinci bir hareketi gerçekleştirir ve verilerin yok olmasına sebep olursa, bu durumda bu neticeden bağımsız olarak TCK md. 243/1 oluşacak ve ayrıca TCK md. 244 gündeme gelecektir. Örneğin bir şirketin hemen dışına park eden hacker evvela şirket ağının WAN erişimine açık kısmına yetkisiz erişir, oradan bir şekilde firewall ve LAN'lar arasındaki router geçişlerini de aşarak şirketin iç ağına bağlanır, buradan da şirketin insan kaynakları biriminin bilgisayarına sızar ise bu durumda sadece TCK md. 243/1 gündeme gelecektir. Aynı failin insan kaynaklarındaki bilgisayara ağ üzerinden yaptığı yetkisiz erişim sürerken şirket binasına girmesi durumunda, fail zaten yetkisiz eriştiği bilgisayarın fişini çeker ise indirme yapan açık bilgisayarın uçucu hafızasındaki veriler silineceğinden, TCK md. 243/1'den bağımsız olarak ayrıca TCK md. 244/2 oluşacaktır.

TCK md. 243/3 nazarında önemli olan bir diğer konu ise ağırlaşan netice yönünden gereken illiyet bağıdır. Uygulamada neticesi sebebiyle ağırlaşmış suçlar yönünden şart teorisi + objektif isnadiyet[452] ve ayrıca uygun sebep teorilerinin[453] kullanılabildiği görülmektedir. Eğer sisteme erişmeye veya sistemde kalmaya yönelik fiil ile sistemdeki yok olan ya da değişen verilere dair netice arasında illiyet bağı kurulamıyor ise bu durumda TCK md. 243/3 değil, birinci veya suçun konusuna göre ikinci fıkra tatbik edilecektir.

TCK md. 243/3'ün objektif tipikliği nazarında önemli olan son husus ise suçun konusuna bağlı olarak oluşan hafifletici sebebin bu durumda uygulanıp

---

[451] Bu konuda ayrıca bkz. Teemu VAİSANEN, Lorena TRİNBERG ve Nikolas PİSSANİDİS 2016, age. s. 30.

[452] Yargıtay CGK 2017/12-271 E. 2017/278 K., İçinde, Berrin AKBULUT 2018, age. s. 315.

[453] Yargıtay CGK 2008/1-186 E. 2009/147 K., İçinde, Mehmet TAN (2011), TCK Genel Hükümler Kırmızı Kitap Cilt 1, Seçkin, Ankara, s. 619 / Yargıtay ölüm neticeli yaralama suçlarında genellikle yaralama fiilinin bizatihi ölüm yönünden elverişli/uygun bir sebep olması durumunda fail yanlış tedavi gibi üçüncü etkenler sonucu ölür ise illiyet bağını var saymaktadır. Bkz. Yargıtay 1. CD 2005/532 K., İçinde; Tan, age. s. 715, 716, 717 / Yargıtay bu konuda elverişliliği geniş çerçeveli yorumlamakta ve dağ başındaki bir köyde hastaneye geç gidilebiliyor olmasını da öngörerek, bu tür gecikmeler dahilinde elverişlilik değerlendirmesi yapmaktadır. Bkz. 1. CD 1994/561 E. 1994/567 K, İçinde, Tan, age. s. 753.

uygulanmayacağıdır. Doktrinde, içerisindeki veriler yetkisiz erişim suçuna konu seçimlik hareketler sonucu yok olan veya değişen bilişim sistemi eğer ikinci fıkradaki hafifletici sebep içerisinde değerlendirilen türde bedeli karşılığı yararlanılan bir sistem ise bu durumda direkt olarak TCK md. 243/3'ün uygulanacağı ve ikinci fıkradaki indirimin söz konusu olmayacağı belirtilmektedir.[454]

3.5.2.2. Sübjektif Tipiklik Yönünden Değerlendirme

Neticesi sebebiyle ağırlaşmış suç tiplerine dair düzenlemelerde ağırlaşmış neticeyi meydana getiren fiili tipikliği içinde barındıran bir temel norm bulunur. TCK md. 243/3 yönünden bu norm TCK md. 244/2'dir.[455] TCK md. 243/3'te düzenlenen neticesi sebebiyle ağırlaşmış suçun oluşabilmesi için kast + taksir kombinasyonu gerekir. Öyleyse failin ancak kasten erişilen sistemde, erişime dair fiilleri nedeniyle gerçekleşen ağırlaşan neticelere yönelik taksir derecesinde bir bilincine sahip olması durumunda TCK md. 243/3 gereğince sorumlu tutulabilecektir.[456]

Taksirde özen yükümlülüğünün değerlendirilmesi objektif kıstaslar dahilinde yapılır. Bu durum normun gerekçesinde belirtildiği gibi doktrindeki genel eğilim de bu yöndedir.[457] Özen yükümlülüğü objektif olarak değerlendirildikten sonra yükümlülüğe aykırılık ortaya konulabiliyor ise taksirin varlığı için ayrıca neticenin sübjektif olarak öngörülebilir olup olmadığı tartışılmalıdır. Türk ceza hukukunda sübjektif sorumluluk esası geçerli olduğundan, failin bu neticeyi sübjektif olarak öngörebilme imkanı yok ise taksir derecesinde dahi bir sorumluluğunun oluşmayacağı unutulmamalıdır.[458] Böyle bir durumda fail yalnızca öngördüğü ve gerçekleşmesini istediği neticeden sorumlu tutulabileceği için salt TCK md. 243/1 gereğince sorumluluğu doğacaktır. Neticesi sebebiyle ağırlaşmış suçlarda suçun temel halinden

---

[454] Ali KARAGÜLMEZ 2014, age. s. 215; Murat Volkan DÜLGER 2022, age. s. 285; Berrin AKBULUT 2017, age. s. 149.

[455] Nazmiye ÖZENBAŞ 2012, age. s. 8.

[456] Murat Volkan DÜLGER 2022, age. s. 276, 277; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 247; Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 962; Ali PARLAR ve Muzaffer HATİPOĞLU 2010, age. s. 3746; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 905; Ali KARAGÜLMEZ 2014, age. s.212, 213; Berrin AKBULUT 2017, age. s. 149.

[457] Veli Özer ÖZBEK 2010, age. s. 275; İzzet ÖZGENÇ 2021, age. s. 259; Fatih Selami MAHMUTOĞLU ve Serra KARADENİZ 2017, age. s. 328; Ayrıca bkz; Nevzat TOROSLU ve Haluk TOROSLU 2021, age. s. 238, 239.

[458] Yargıtay 12. CD 2011/15869 E. 2012/5011 K. İçinde, İsmail MALKOÇ (2013), *Açıklamalı Türk Ceza Kanunu Cilt 1*, Ankara, s. 296, 297 / Ayrıca bkz. Erdener YURTCAN (2015), *Türk Ceza Kanunu Genel Hükümler Cilt 1*, TBB Yayınları, Ankara, s. 342.

ağır bir yaptırım uygulandığından, bu suç tiplerinde ayrıca bilinçli taksire yönelik bir ceza artırımı yapılmaz.[459]

3.5.2.3. Hukuka Aykırılık Yönünden Değerlendirme

TCK md. 243/3'te düzenlenen neticesi sebebiyle ağırlaşmış suç tipinde, korunan hukuki değerlerin suçun temel halinden farklılaştığı görülmektedir. İlgili alt başlık altında zikredildiği üzere suçun temel hali verilerin bütünlüğünü koruma amacı gütmemektedir. Korumayı amaçladığı hukuki değerler verilerin bütünlüğü olan esas suç, TCK md. 244/2'de düzenlenmiştir. TCK md. 243/3'ün korumayı amaçladığı değerler de verilerin bütünlüğü açısından TCK md. 244/2 ile birleşmekte, TCK md. 243/1'den ise ayrışmaktadır.[460]

TCK md. 243/3'te düzenlenen neticesi sebebiyle ağırlaşmış suçun varlığında, gerçekleşmesi istenilen esas netice salt sisteme erişmek/kalmaya devam etmek olmakla birlikte, istenmeden verilerin yok olmasına veya değişmesine sebep olunmaktadır. Böyle bir durumda bu istenmeyen netice gerçekleşmemiş olsaydı hukuka uygun sayılacak bir fiilin, ağırlaşan neticeye sebep olunması durumunda da hukuka uygun sayılıp sayılmayacağı meselesi gündeme gelmektedir. Doktrinde, gerçekleştirilmesi istenilen netice oluşsa idi hukuka uygun bir durum oluşacaktı ise ağırlaşan netice yönünden de fiilin hukuka uygun sayılacağı belirtilmektedir.[461]

Böyle bir durumun özellikle sızma testleri sırasında yaşanması muhtemeldir. Örneğin sözleşmede buna yönelik bir sorumsuzluk şerhi düşülmemiş ise rıza ile yapılan sızma testi sırasında sistemdeki verilerin yok olması ya da zarar görmesi durumunda TCK md. 243/3 yönünden bir hukuka aykırılık gündeme gelmeyebilir. Böyle bir hukuka uygunluğun gerçekleşebilmesi için sisteme erişim ve kalmaya devam etmeye dair hukuka uygunluk sebebini oluşturan gerekçelerin kapsamının aşılmaması gerekir. Örneğin sızma testi konusunda sözleşme hükümleri ile verilen rıza hukuka uygunluk sebebidir. Şekle bağlı olmayan sızma testi sözleşmesinin içeriğinin detaylı olması gerekmese de sızma testi sonucu verilere istenmeden zarar verilmiş ise rıza direkt olarak bu sızma testini hukuka uygun kılmaz. İstenmeyen ağır neticenin oluşumu durumunda, fiilin hukuka uygunluğu için belirli standartlara uygun ve özen

[459] Koray DOĞAN 2015, age. s. 236; Nazmiye ÖZENBAŞ 2012, age. s. 348.
[460] Veriler üzerindeki mülkiyet hakkı yönünden benzer yorumlar için bkz. Tunç DEMİRCAN 2007, age. s. 85.
[461] Veli Özer ÖZBEK 2010, age. s. 520.

yükümlülüğü ihlal edilmeden gerçekleştirilmiş bir testin varlığı gerekir. Yine örneğin CMK md. 134 bağlamında yapılan bir arama sırasında gerçekleştirilen işlemler sonucu veriler istenmeden yok edilir ya da değiştirilir ise kanun hükmünü(*md. 134*) icra direkt olarak neticesi sebebiyle ağırlaşmış suç yönünden bir hukuka uygunluk sebebi teşkil etmez. Bunun için aramayı yapan görevlilerin yine görev tanımı içerisindeki standart işlemleri gerçekleştirmiş ve normal şartlar altında bir kolluk ya da adli bilişim görevlisinin yapmaması gereken bir işlemi gerçekleştirmemiş olması gerekir.

BÖLÜM IV

ARAYA GİRME SUÇUNUN UNSURLARI

4.1 NORMUN KORUMAYI AMAÇLADIĞI HUKUKSAL DEĞERLER

4.1.1. Normun Yürürlüğe Konuluş Şekli ve Bunun Korunması Amaçlanan Hukuksal Değerler ile Bağlantısı (*Kişisel Veriler*)

TCK md. 243/4'te düzenlenen araya girme suçu, doğru olmayan bir şekilde 6698 s. Kanun ile yürürlüğe girmiş ve TCK'ya eklenmiştir. Neden ''torba kanunlar'' ile ya da spesifik olarak TCK'da değişiklik yapan bir kanun ile yürürlüğe sokulmadığı anlaşılamayan bu normun 6698 s. Kişisel Verilerin Korunması Kanunu içerisinde yürürlüğe sokulup bilahare TCK'ya işlenmesi sanki bu normun korumayı amaçladığı değerin kişisel veriler olduğu gibi yanlış bir izlenim doğurmaktadır. Bilişim sistemleri arasında akan veri trafiğinin hiçbir kişisel veri barındırmaması pekala çoğu durumda mümkündür. Veri trafiği izlendiği sırada verilerin içerdiği bilgilere ve hatta kriptografik kodlamalara da zaten çoğu zaman erişilemeyebilir. Ayrıca trafiğe dair genel bilgiler yani örneğin gönderici-alıcı taraflara dair IP ve zaman bilgisi de iletişimdeki sistemler kişisel kullanıma ait değilse, birer kişisel veri sayılmayacaktır. Öyleyse normun korumayı amaçladığı değerler arasında kişisel veriler ve hatta verilerin içerdiği bilgiler yer almamaktadır.

4.1.2. Doktrin Görüşleri ve Değerlendirme

Doktrinde bir görüşe göre bu suç ile korunan hukuki değerler bilişim sistemlerinin güvenliği, güvenilirliği ve veri iletişiminin mahremiyetine dair hakkın korunmasıdır.[462] İkinci bir görüşe göre ise suçla korunan hukuki değer

[462] Mehmet Bedii KAYA 2019, age. s. 242.

veri güvenliğidir.[463] Diğer bir görüş ise bu suç ile bilişim sistemlerinin güvenliğinin ve ayrıca özel hayatın gizliliğinin korunduğunu belirtmektedir.[464] Dördüncü görüş ise bu norm ile korunması amaçlanan değerin, veriler üzerinde tasarruf yetkisi olanların verilerin iletimindeki gizliliğe dair beklentisi/hakkıdır.[465] Araya girme suçunun ASS'deki karşılığı olan üçüncü maddeye dair ASS Açıklayıcı Rapor'da da suçun veri iletişiminin mahremiyetine dair hakkı korumayı amaçladığı, iletilen veriler kamuya açık bilgiler içermekte olsa bile iletişim kamuya açık biçimde yapılmıyor ise bu iletişimi izlemenin normun korumayı amaçladığı değerleri ihlal edeceği yazılıdır.

Kanaatimizce bu suç normu ile korunan tek hukuki değer, ''veri trafiğinin gizliliğine'' dair haktır. Elektronik haberleşme teknolojileri ile her daim iki insanın birbiri ile mesajlaşması ya da dosya iletimi söz konusu olmadığı ve insan-sistem(*örn. bir internet kullanıcısının uygulama sunucusuna veri iletmesi*) ya da sistem-sistem(*örn. IoT cihazların kendi aralarındaki trafik*) haberleşmesi ve veri iletişimi gerçekleşebildiğinden, haberleşmenin gizliliğine dair hak, bu suç ile korunan bir değer değildir.

Belirtmek gerekir ki elektronik haberleşme kablolar ya da elektromanyetik dalgalar üzerinden yapılırken veri iletişim kanallarında bu veriler gizlenemez ve ancak trafik yahut verilerin içerdiği bilgiler kriptolanabilir. Bu sebeple veri paketlerini yakalayacak teknolojilerden gizlenmesi mümkün olmayan elektronik haberleşmede, akan veri trafiğinin her daim üçünü kişilerden gizli olduğuna dair haklı bir beklenti mevcuttur. Bu durum tıpkı çalışır vaziyette kapısı açık bir arabanın öylece alınıp götürülememesine benzer. İşte normun korumayı amaçladığı tek değer bu meşru beklenti yani veri iletişiminin/trafiğinin gizliliğine dair haktır.[466]

4.2. SUÇUN TİPİKLİK UNSURU

4.2.1. Objektif Tipiklik

4.2.1.1. Fail

TCK md. 243/4'te yer alan araya girme suçunda özgü failliğe dair herhangi bir düzenleme bulunmamaktadır. Bu sebeple suçun faili herkes olabilir.[467] Burada önemsenmesi gereken husus, bu suçun failinin veri trafiğini/nakillerini ''iletişimin

[463] Murat Volkan DÜLGER 2022, age. s. 322; Nagihan GÜN 2020, age. s. 206.
[464] Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1162.
[465] Berrin AKBULUT 2017, age. s. 159.
[466] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 908.
[467] Berrin AKBULUT 2017, age. s. 159, 160; Murat Volkan DÜLGER 2022, age. s. 322.

alıcı-verici taraflarındaki sistemlere erişmeden'' teknik araçlar ile izleyen kişi olduğudur. Aynı fail bu izleme işlemini üçüncü taraf bir bilişim sistemine sızarak mitm konumunda da gerçekleştirebilir. Eğer fail bu üçüncü taraf sisteme yetkisiz olarak erişmiş ise burada ayrıca yetkisiz erişim suçu yönünden de fail sıfatına sahip olacaktır. Fakat bu üçüncü taraf sisteme yönelik fiilleri sebebiyle TCK md. 243/4 yönünden fail sıfatı doğmaz. Örneğin fail WAN ile kurum VLAN'ı arasında trafiği filtreleyen proxy sisteme sızmış ve VLAN'daki X makinesi ile WAN'daki istemci arasındaki veri paketlerini bu iki sisteme de erişmeden, sızdığı proxy üzerinden yakalayarak izlemiş ise hem TCK md. 243/1 hem de 243/4'den ayrı ayrı fail konumunda bulunacaktır.

4.2.1.2. Mağdur

Araya girme suçunda mağdur yönünden de herhangi bir özel durum bulunmayıp, herkesin bu suçun mağduru olması mümkündür. Suçun konusu salt gerçek kişilere özgü veriler olmadığından, tüzel kişilere dair veri trafiğinin de araya girilerek izlenmesi/dinlenmesi mümkündür. Tüzel kişilerin bir suçun mağduru olup olamayacağına dair benimsenecek görüşlere göre tüzel kişilerin bu suçtaki mağdur sıfatını takdir etmek gerekir. Bu konuda detaylı açıklamalar ve şahsi görüşümüz için tezin yetkisiz erişim suçunun unsurlarının aktarıldığı kısımlarına bakılmalıdır.

Doktrinde araya girme suçunda kimin mağdur olarak nitelendirilebileceği noktasında farklı görüşler mevcuttur. Bir görüşe göre izlenen/dinlenen trafikteki veriler ile ilgisi olanlar mağdur olarak nitelendirilmelidir.[468] Diğer bir görüşe göre ise trafikteki veriler üzerinde tasarruf ve hak sahibi olanlar mağdurdur.[469] Benzer bir görüş, bu suçta mağdurun yalnızca verilerin öznesi olan kişi olduğu yönündedir.[470] Sair bir görüşe göre ise bu suçta mağdur, veri trafiği izlenen kişi ve ayrıca sistemin sahibidir.[471]

Kanaatimizce yetkisiz erişim suçu gibi araya girme suçunda da temel olarak verilerin anlam kazanmış biçimi olan bilgiler, normun koruma amacı dışındadır. Pek çok ağ yapısında, iki veya daha çok sistemin bir arada yaptığı iletişime konu veriler ne bir kişisel veri ne de iletişimin tarafları ile en ufak bağlantısı bulunan bilgiler değildir. ASS Açıklayıcı Rapor'da da sözleşmenin üçüncü maddesine yönelik, iletilen verilerin kamuya açık bilgilere dair olabileceği lakin iletişimin kamuya açık olmaması

[468] Murat Volkan DÜLGER 2022, age. s. 323.
[469] Berrin AKBULUT 2017, age. s. 160.
[470] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 909.
[471] Ahmet GÜL 2021, age. s. 95.

durumunda bunun suça konu bir durum yaratacağı belirtilmektedir. Bu doğrultuda örneğin otobüs saatlerinin ve otobüslerin güncel konumunun verildiği bir uygulama yazılımına konu verileri barındıran sunucu ile uygulamayı kullanan istemci sistem arasındaki veri trafiği izlendiğinde, şüphesiz ki verilere yönelik bilgiler ile ilgisi bulunan kişinin yani otobüsleri işleten belediyenin mağdur sıfatına sahip olmaması gerekir. Aynı şekilde öğrencilerin sınav kağıtlarının taranmış veri dosyası hallerinin üniversite CAN'ı üzerindeki X sisteminden Y sistemine nakli sırasında, bu trafik ağdaki Z sistemi üzerinden izleniyor ise bu durumda da sınav kağıtlarının sahibi öğrencilerin mağdur sıfatı gündeme gelemez. Burada öğrenciler olsa olsa kişisel verilere dair suçların mağduru olabilirler. Zaten veri trafiğinin araya girilerek izlenmesi durumunda, ilk etapta iletişim halindeki sistemlerin ''dar anlamdaki trafik bilgisi'' yani sistem bilgileri(*IP, port vb.)* ile gönderim/iletim zamanları ve gönderimdeki veri paketlerinin yalnızca teknik kodlamalar olan paket başlıkları görülebilir. Veri paketlerinin içeriğinin öğrenilebilmesi için paketleri yakalamada kullanılan yazılımın ayrıca paket içeriğini görebilecek bir yetkinliğe de sahip olması ve bu yetkinliğin de fail tarafından kullanılması gerekir. Öyleyse TCK md. 243/4'te düzenlenen araya girme suçunun işlenmesi durumunda nakil halindeki verilerin içerdiği bilgilerin kimler ile ilgili oldukları ya da verilerin öznesi çoğu zaman zaten öğrenilemez.

Yukarıdaki açıklamalar dolayısıyla kanaatimizce araya girme suçunda mağdur sıfatının, yalnızca veri trafiğinin taraflarında bulunması gerekir. Her ne kadar veri paketleri yakalandığında verilerin kimden gelip kime gittiğine dair IP-port vb. bilgi elde ediliyor ve bu bilgiler de iletişimin tarafı kişilerden ziyade sistemlerin kimlikleriyle ilgili ise de bu suçun mağdurunun iletişimdeki sistemlerin sahipleri olmadığını düşünüyoruz. Suçun mağduru, iletişimde kullandığı sistem üzerinde genel yetki sahibi olsun ya da olmasın, iletişimi dinlenen/izlenen kişi yani iletişimin tarafıdır. Örneğin arkadaşının bilgisayarından bir mail yollamak için izin alan kişinin maili, alıcı Y'ye iletilmeden mail sunucusuna sızmış hacker tarafından izlenmiş ise bilgisayarın sahibinin mağdur sıfatına sahip olmaması gerekir. Böyle bir durumda TCK md. 243/4 yönünden mağdur, gönderici ve alıcı taraflar olabilir. Aradaki mail sunucuya dair ise şartları mevcut ise TCK md. 243/1 yönünden servis sağlayıcının mağdur sıfatı gündeme gelebilecektir.

4.2.1.3. Suçun Konusu

Doktrindeki genel kanaat, suçun konusunun iletim/nakil halindeki veriler olduğudur.[472] Doktrindeki görüşlere göre birden fazla sistem arasındaki veya bir sistemin kendi içerisindeki nakil halindeki veriler bu suçun konusunu teşkil edecektir.[473] Her ne kadar TCK md. 243/4'ün lafzında, ''*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında …*'' denilmiş ve bu suçun ASS'deki karşılığı olan sözleşmenin üçüncü maddesinde,

> ''*…bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak gerçekleştirilen araya girme fiilinin, …*''

denilmiş ise de bu düzenlemelerde yer alan ''*bir bilişim sisteminin kendi içerisindeki veri nakilleri*'' kavramı kapalı bir anlam taşımaktadır.

Bu düzenlemelerden sanki tek bir sistemin kendi içerisindeki veri nakilleri ve örneğin bilgisayardaki bir dosyanın bir klasörden diğerine gönderiminin bir şekilde bilgisayara erişmeden teknik araçlarla izlenmesi durumunun da suçun tipikliği içerisinde kalacağı izlenimi oluşmaktadır. Halbuki bu suçtan anlaşılması gereken husus bu değildir. Suçun konusunu oluşturabilecek veriler, yalnızca bir ağ içerisinde iletişim kuran iki veya daha fazla sayıdaki farklı bilişim sistemleri arasındaki iletişime konu verilerdir.[474] Sanıyoruz ki ilgili normlarda ''*bir sistemin kendi içerisindeki veri nakilleri*'' tabiri ile anlatılmak istenen, içerisinde bulunan bağlı sistemlerden ayrık olarak bilişim sistemi sayılan LAN ağlarındaki kapalı devre veri trafiğinin izlenmesidir ve örneğin bir ev içerisindeki wi-fi modem ile veri gönderen bilgisayarın arasındaki iletişimdeki veriler, TCK md. 243/4'teki suçun konusunu oluşturacaktır.[475]

Suçun konusunu oluşturan verilerin internet teknolojilerine dair ağ yapılarında nakledildiyor olması şart olmayıp, bluetooth ve sair her türlü ağ yapısının içerisindeki trafiğe dair veriler bu suçun konusudur. Aynı şekilde her türlü M2M-IoT teknolojisi yönünden eğer haberleşen minimum iki ayrı bilişim sistemi mevcut ve bu sistemler tek bir makinenin/aletin üzerinde konumlandırılmış ise bu durumda da makine içerisindeki

---

[472] Murat Volkan DÜLGER 2022, age. s. 323; Berrin AKBULUT 2017, age. s. 160, 161.
[473] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 909; Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1162.
[474] Benzer yönde bkz. Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. s. 1162.
[475] Örneğin doktrinde Dülger, tek bir bilişim sistemi içerisindeki veri nakillerini bu şekilde printer-bilgisayar arasındaki veri iletişimini örnek göstererek açıklamaktadır. Bkz. Murat Volkan DÜLGER 2022, age. s. 324.

ayrı bilişim sistemlerinin arasındaki haberleşmeye dair veriler bu suçun konusunu oluşturacaktır. Örneğin bir endüstriyel robotun üzerinde pek çok farklı sistem, birlikte entegre bir ağ yapısı oluşturmuş olabilir. Böyle bir durumda robotun kendi içindeki ağ yapısı üzerinde haberleşen farklı sistemlerin iletişimindeki nakil halindeki veriler, TCK md. 243/4'ün konusunu teşkil edecektir.

4.2.1.4. Fiil ve Netice

Araya girme suçunun objektif tipikliğine konu fiil, veri nakillerini ''iletişimin tarafı sistemlere erişmeksizin'' teknik araçlarla hukuka aykırı olarak izlemektir. İzleme devam ettiği sürece suç temadi edeceğinden, doktrinde araya girme suçunun mütemadi/kesintisiz bir suç olduğu zikredilmektedir.[476] Kanaatimizce kanun koyucu aksi yönde bir düzenleme öngörmediği için veri paketlerinin yakalanması ve analizine yani trafiğin izlenmesine dair netice gerçekleştiği an suç tamamlanacak, izleme devam ettiği sürece suçun işlenmesi devam edecektir. Neticenin oluşumu yönünden belirli bir sürenin geçmesi şartı aranmadığından, teoride ani suç olarak işlenebilen bu suç yönünden, ''muhtemel'' mütemadi suç[477] nitelemesi yapmak daha doğru olacaktır. Araya girme suçunun objektif tipikliğine konu fiillerin, normun lafzında açıkça belirtildiği üzere sisteme girmeksizin/erişmeksizin gerçekleştirilmesi gerekir. Açıkça yazılı olmasa da TCK md. 243/4'e konu fiilin oluşabilmesi için erişilmemesi gereken sistemler, iletişimin gönderici-alıcı tarafı olan bilişim sistemleridir.[478]

Neticesi harekete bitişik bir suç olan araya girme suçunun oluşumu yönünden veri trafiğine dair genel bilgilerin yahut nakil halindeki verilerin hangi bilgileri içerdiğinin öğrenilmesi gerekmez. Böyle bir neticenin doğumunda ayrıca haberleşmenin gizliliğini ihlal ya da kişisel verilerin ele geçirilmesi gibi sair suçların da oluşması gündeme gelecektir.[479] Örneğin failin VPN, SSL, TOR ve sair teknolojiler vasıtasıyla kriptolanmış bir trafiği araya girerek izlemesi durumunda, fail eğer

---

[476] Berrin AKBULUT 2017, age. s. 169 / Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 910; Murat Volkan DÜLGER 2022, age. s. 326; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 247.

[477] Muhtemel mütemadi suçlara dair açıklamalar için bkz. Erdal YERDELEN 2014, age. s. 117, 118.

[478] Her ne kadar normun lafzında '' *veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen*'' denilmiş ise de girilmemesi/erişilmemesi gereken sistemler yalnızca iletişimin gönderici-alıcı tarafındaki sistemler olarak anlaşılmalıdır. Aksi halde bu suç işlenemez bir suç olacağı gibi pratikte gerçekleşen mitm ve sniffing saldırıları da cezalandırılamayacak, normun amacı tecelli edemeyecektir. / Alman Ceza Kanunu StGB md. 202b'de TCK md. 243/4'te düzenlenen araya girme suçunun eşleniği olan suç normunun lafzında ''failin veri paketleri yakalanan iletişimin tarafı olmaması gereği'' açıkça zikredilmiştir.

[479] Berrin AKBULUT 2017, age. s. 165.

kriptoyu kıracak anahtarı bilmiyorsa, bu faaliyetlerinden anlamlı bir bilgi elde edemez. Mesela istemciden abcd.org/abcdabcd URL adresine x boyutunda veri paketleri gönderilir lakin araya giren fail kriptolanan bu trafik bilgisini göremez. Aynı şekilde verilerin içerdiği mesajdaki ‘’merhaba‘’ yazısı da araya giren fail tarafından ‘’xas2310920sxsa‘’ gibi kriptolanmış biçimde görülür. Fail kriptoyu çözerek trafiğe dair genel bilgilere yahut verilerin içerdiği esas bilgilere ulaşamasa bile salt veri trafiğini izlemiş olması sebebiyle TCK md. 243/4'te düzenlenen araya girme suçu oluşacaktır.

Veri nakillerinin izlenmesi sonucunda, yakalanan ‘’veri trafiğine‘’ dair genel bilgilerin öğrenilmesi ile ‘’verilerin içerdiği‘’ esas bilgilerin öğrenilmesi arasındaki farkın kavranması önemlidir. Nakil halindeki veriler somut bir varlık olmadığından, teknik araç vasıtasıyla da olsa bir kuşun uçması ya da trenin geçişi gibi göz ile görülebilecek şeyler değildir. Nakil halindeki verilerin araya girilerek izlenmiş olması için veri trafiğine dair genel bilgilerin, paket analiz yazılımını çalıştıran bir cihaz vasıtasıyla kriptolu veya kriptosuz biçimde öğrenilmesi gerekir ki suça konu temel netice de budur.[480]

Veri paketleri yakalandığında, kullanılan paket analiz yazılımının yetkinlik derecesine göre bu trafiğe dair çeşitli bilgiler elde edilebilecektir. Örneğin standart bir yazılımın kullanımında; paket başlıklarına dair yalnızca komutlar, verilerin boyutu, hangi tür bir veri gönderildiği, gönderici ve alıcı sistemlere dair IP, port, iç ağda MAC adresi ile işletim sistemi ve sair sistem bilgileri ve ayrıca gönderim saati gibi genel bilgiler elde edilir. Daha üst seviye yazılımlar ise verilerin hangi uygulama yazılımı vasıtasıyla gönderildiğine, URL bilgisine ve alıcı mail adresine dair bilgi ile trafiğe dair sair bilgilerin görülebilmesini sağlar. Bu durumlar bir telefon görüşmesinde; konuşmanın hangi telefonlar, hangi sim kartları arasında ve ne zaman, kaç dakika yapıldığının bilinmesine fakat konuşmaların dinlenmemesine benzer. Daha üstün teknolojiler ise veri trafiğine dair bilgilerin yanında verilerin içeriğindeki bilgilere ve örneğin mesaj ya da gönderilen veri dosyalarının içeriklerine yahut VoIP görüşmelerindeki konuşmalara da ulaşılmasını sağlayabilir. İşte bu ikinci tip neticeler, nakil halindeki veri paketlerinin genel bilgilerinin yani trafik bilgisinin değil, verilerin içerdiği ‘’esas bilgilerin‘’ öğrenilmesidir. Bu durum ise telefon görüşmesinde konuşmaların da dinlenmiş olmasına benzer.

[480] Bu konuda Wireshark yazılımını örnek göstererek suça konu fiili açıklayan benzer yöndeki görüşler için bkz. Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 242.

4.2.1.4.1. Suçta Kullanılabilecek Teknik Araçlara Dair Değerlendirme

Suça konu fiilin oluşabilmesi için normun lafzında ‘’teknik araçla‘’ denildiği için veri trafiğinin izlenmesinin teknik araç vasıtasıyla yapılması şarttır.[481] Bu sebeple iletişimin tarafı olan bir sistemin başına gidilerek göz ile trafiğe konu verilerin izlenmesi durumunda suça konu fiil oluşmayacaktır. Lakin her türlü teknik araç, bu suçun objektif tipikliği içerisinde değerlendirilemez. Zira suçun gerek ASS'de gerekse TCK'da düzenleniş biçimi, mitm ve sniffing gibi bu yöndeki tipik hacking saldırılarının ‘’*iletişimdeki sistemlere erişilmeden gerçekleştirilmesi*‘’ durumunda bir kanun boşluğu doğamaması amacına yöneliktir. Bu sebeple normun korumayı amaçladığı değeler veri trafiğinin her türlü teknik araç vasıtasıyla izlenmesi değildir.

Teknik araç kavramının normatif bir tanımı yoktur. Elektrikli bir dürbünün dahi hukuken teknik araç sayılması ve kişinin dürbünle ya da güçlü bir teleskop ile perdesiz camların arkasındaki sistemlerdeki veri nakillerini ekrandan izlemesi mümkündür. Ancak böyle bir eylem TCK md. 243/4'ün objektif tipikliği içerisinde değerlendirilmemelidir. Aynı şekilde gizli olarak ekranı kameraya çekilen bir bilgisayarın internet üzerinde gerçekleştirdiği işlemler ve diğer sistemler ile yaptığı iletişim, kamera kaydının bilahare izlenmesi suretiyle sisteme erişmeden teknik araçla izlenebilir. İşin içine hackingin de girdiği sair bir ihtimalde ise kişinin akıllı televizyonu hacklendikten sonra televizyona bağlı kamera üzerinden tam karşıdaki bilgisayarın ekranı da gözlenebilir. Bu tür durumlar teknik araçlarla veri nakillerini izlemek olsa da bu tür teknik araçların TCK md. 243/4 nazarında değerlendirilmesi mümkün olmamalıdır. Kanaatimizce TCK md. 243/4'te kullanılabilecek bir teknik aracın, kablolar ya da elektromanyetik dalgalar üzerinden iletilen veri paketlerini yakalayabilecek ve bu sayede veri trafiğini izlemeyi gerçekleştirecek bir cihaz olması şarttır. Suçta kullanılacak teknik aracın kablolar ya da elektromanyetik dalgalar üzerinden iletilen veri paketlerini yakalayabilecek ve bu sayede veri trafiğini izlemeyi gerçekleştirecek bir cihaz olması zorunluluğundan bir şart daha doğmaktadır. Bu ikinci şart da teknik araçlar ile veri nakillerinin izlenmesi eyleminin iletişimin tarafı bilişim sistemlerinin ekranları değil, iletişim hatları yani elektronik haberleşme omurgası üzerinden gerçekleştirilmesi gerektiğidir.[482]

[481] Murat Volkan DÜLGER 2022, age. s. 325.
[482] Suça konu fiilin ağdaki veri akışını izlemek olduğu şeklindeki benzer görüşler için bkz. Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 962.

4.2.1.4.2. İzleme Fiilinin Anlamı ve Örnekler

Doktrinde ‘’izleme‘’ fiilinin 5651 s. Kanun md. 2/1-h’deki tanımlama ile açıklandığı görüşler mevcuttur.[483] İlgili tanım ‘’*İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesi*‘’ şeklinde olup, bu tanım aslında aynı kanunun 10. maddesinde BTK’ya verilen ön alan araştırması yapma görevi ile ilgilidir. İlgili maddede zikredildiği üzere bu ‘’izleme‘’ belirli suç tipleri ile ilgili olarak internet ortamındaki aleni ortamların izlenmesine yöneliktir. Buradaki izleme faaliyeti esasında sanal devriyeler yani herkesin erişebildiği internet site ve uygulamaları üzerindeki, ekranda gözle görülen sanal ortamın izlenmesidir. Erişim sağlayıcıların zaten tutmakla yükümlü oldukları trafik bilgisinin bu sanal devriyeler sonucu ulaşılan sonuçlar ile ilişkilendirilebilmesi yönünden ise BTK’nın izleme faaliyetlerine dair trafik bilgisine erişimine yönelik ek bir düzenleme getirilmiştir.[484] TCK md. 243/4’ün objektif tipikliğine konu veri nakillerine yönelik izleme fiili ise sanal devriyeler ile bağlantısız bir eylemdir.

TCK md. 243/4’e konu bir izlemede, internet ya da intranet site/uygulamalarının kullanıcı ara yüzleri üzerinde görülen somutlaşmış bilgi halindeki veriler değil, internet ya da intranet ağları içerisindeki gözle görülmeyen, omurga üzerinde akan trafiğe konu veriler izlenir. Bu trafiğe konu veri iletişimi nihayete erer ve iletişimin sunucu tarafı eğer iletişime konu bilgileri site/uygulamanın kullanıcı ara yüzü üzerinde yayınlar ise bu durumda iletişimdeki veriler artık durağan hale gelmiş ve site/uygulama üzerinden gözle görülebilir olmuş olur. Lakin sunucunun verileri yayınlaması durumunda dahi veri trafiğinin izlenmesi ile görülecek bilgiler, yayınlanan verilere dair bilgilerden farklı olacaktır. Konunun daha net anlaşılabilmesi için aşağıda iletişimin tarafı olan sistemlere girilmeden/erişilmeden, sistemler arasındaki veri nakillerinin nasıl izlenebildiği/dinlenebildiği çeşitli örnek çerçeve durumlar üzerinden açıklanmıştır.

---

[483] Murat Volkan DÜLGER 2022, age. s. 325.

[484] Her ne kadar 5651 s. Kanun’dan bu yönde bir anlam çıkartmaya yönelik açık düzenleme yok ise de İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik md. 8 ve ayrıca Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik md. 15’te erişim sağlayıcıların internet trafiğine dair trafik bilgilerini kaydetme yükümlülüğü düzenlenirken, ‘’*Başkanlığın 5651 sayılı Kanunla verilen görevleri yerine getirebilmesi için yapacağı trafik izlemesinde Başkanlığa gerekli yardım ve desteği sağlamakla*‘’ yükümlü olduğu da zikredildiğinden, BTK’nın bu izleme faaliyetinin erişim sağlayıcıların tuttuğu trafik bilgileri ile bağlantılı bir yönü de mevcut olmaktadır.

1) İletişimin istemci-sunucu(*gönderici-alıcı*) tarafları olan bilişim sistemlerine erişmeksizin iletişimdeki veri trafiğini teknik araçlarla izlemenin ilk yolu, mitm konumundaki ara sistem üzerinden veri paketlerini yakalamaktır.[485] Mitm konumundaki ara sistemler, istemci-sunucu arasındaki iletişimde verilerin üzerinden geçtiği ve bu şekilde nihai sunucuya iletildiği sistemlerdir. Birinci ihtimalde fail zaten bu ara sistemler üzerinde meşru yetki sahibi olup, kendi yetkisi altındaki bir ara sistem üzerinde çalıştırdığı paket analiz yazılımı ile bu hukuka aykırı izleme işlemini gerçekleştirir. Örneğin bir şirket VLAN'ının internet erişimine açık kısmında, WAN ile VLAN içerisindeki iletişimi filtreleyebilmesi için proxy konumunda çalıştırılan X bilgisayarı bulunabilir ve trafik ağdaki Z ya da Y bilgisayarına gidecek olsa bile evvela bu X bilgisayarı üzerinden geçiyor olabilir. Böyle bir durumda X bilgisayarını yetkili olarak kontrol eden görevli, görev tanımında olmadığı halde WAN'dan gelen trafiği, ne WAN'daki gönderici sisteme ne de alıcı Z veya Y sistemine erişmeden ara konumda izler ise işte bu durumda TCK md. 243/4'teki fiil/netice gerçekleşecektir. Aynı şirket ağında WAN ile VLAN arasındaki iletişim ayrıca kurulan VPN sunucular üzerinden kriptolu biçimde geçiriliyor ve bunun için de üçüncü taraf bir servis sağlayıcıdan hizmet alınıyor olabilir. Böyle bir durumda WAN'dan gelen trafik VPN sunucuları üzerinden X bilgisayarına, oradan da Z veya Y bilgisayarına aktarılır. Servis sağlayıcı da verdiği hizmeti kötüye kullanır ve izleme işini ara konumdaki VPN sunucular üzerinde gerçekleştirir ise bu durumda da aynı fiil/netice doğacaktır. Kanaatimizce pratikte TCK md. 243/4'e konu fiillerin gerçekleşme alanına dair verilebilecek en somut örnek, sırf bu menfi amaçla kurulmuş ara sistemler ve örneğin kullanıcıların erişime engelli sitelere girebilmek için kullandıkları bedava hizmet veren VPN, Proxy ve DNS servis sağlayıcılar üzerinden bu suçun işlenmesidir.

Bu ara sistemlere bir hacker da sızabilir ve evvela TCK md. 243/1'deki yetkisiz erişim suçunu işleyerek bu sistemlere yetkisiz olarak erişir, bilahare de yetkisiz olarak eriştiği bu sistem üzerinden veri trafiğini hukuka aykırı olarak izleyebilir. Bu durumda hem TCK md. 243/1 hem de TCK md. 243/4'e konu fiil ve neticeler oluşacaktır. Son olarak trafiğin kendi omurgası üzerinden aktığı bir erişim sağlayıcı, omurga üzerine kurduğu sistemler üzerinden veri trafiğini TCK md. 243/4 bağlamında izleyebilir. Bu durum hukukumuzda trafik bilgisi olarak isimlendirilen bir kısım dar manadaki trafik

[485] Bu yöntemin detayları için işbu tezin hacking yöntemlerinin açıklandığı ikinci bölümünün Man In The Middle alt başlığı altına yapılan açıklamalara bakılmalıdır.

bilgisine dair erişim sağlayıcılar yönünden bir yükümlülük olup, erişim sağlayıcıların bu yöndeki fiilleri hukuka uygun olacaktır.

2) İletişimin istemci-sunucu(*gönderici-alıcı*) tarafları olan bilişim sistemlerine girmek/erişmeksizin iletişimdeki veri trafiğini teknik araçlarla izlemenin ikinci yolu, doğrudan ağ trafiğini izlemektir.[486] İlk olarak fail içerisine dahil olduğu bir ağ yapısında, kendi sistemi üzerine kuracağı paket analiz yazılımı ile ağda gerçekleşen veri trafiğini izleyebilir. Kişi ağda hukuka uygun olarak bulunabileceği gibi ağa yetkisiz olarak erişmiş de olabilir ve bu ikinci ihtimalde hem TCK md. 243/1 hem de 243/4'e konu fiil ve neticeler oluşacaktır.

İkinci olarak verilerin elektromanyetik dalgalar üzerinden kablosuz olarak iletildiği bir ağ yapısında, fail ağa dahil olmadan da bu sinyalleri yakalayarak trafiği izleyebilir. Bu faaliyeti sinyalleri yakalayabilen herhangi bir kişi gerçekleştirebileceği gibi çok kapsamlı alıcılar kullanan istihbarat servisleri ya da devletlerin sair organlarının gerçekleştirdiği faaliyetler de mevcuttur. Örneğin Echalon ya da Prism gibi devasa alıcılara sahip sistemler vasıtasıyla, dünya üzerindeki çok geniş coğrafyalarda yapılan veri trafiğinin bu sistemlerin yer aldığı merkezler üzerinden izlendiği/dinlendiği belirtilmektedir.[487] Bu tür durumların Türk hukuku yönünden mümkün olup olmadığı, özellikle MİT Kanunu çerçevesinde aşağıda hukuka uygunluk sebepleri özelinde tartışılmıştır.

3) İletişimin istemci-sunucu(*gönderici-alıcı*) tarafları olan bilişim sistemlerine girmek/erişmeksizin iletişimdeki veri trafiğini teknik araçlarla izlemenin üçüncü yolu, veri paketlerini yakalayacak bir teknoloji kullanmadan, failin iletimdeki verilerin alıcı sistem yerine kendisine gönderilmesini sağlamasıdır. Evvela bu noktada manipülasyona yönelik spoofing yöntemleri ve alıcı IP-MAC-port bilgilerinin taklit edilmesi gündeme gelebilir. Veriler doğrudan kendisine iletileceği için failin burada paketleri yakalaması ve analiz etmesi de gerekmez. Böyle bir durumda yapılan manipülasyon, gönderici/istemcinin ya da ağda veri trafiğini sağlayan protokolleri

[486] Bu yöntemin detayları için işbu tezin hacking yöntemlerinin açıklandığı ikinci bölümünün Sniffing alt başlığı altına yapılan açıklamalara bakılmalıdır.

[487] Fatih TÜRK (2019), *İstihbaratın Teşkilatlanma ve Yönetim Sorunsalı: A.B.D. Örneği*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı Yüksek Lisans Tezi, İstanbul, s. 75, 76, 77, 78 vd; Wikipedia, PRISM, https://en.wikipedia.org/wiki/PRISM_(surveillance_program), (ET: 02.03.2022); Wikipedia, ECHELON, https://en.wikipedia.org/wiki/ECHELON, (ET: 02.03.2022).

işleten sistemlerin bozulmasına sebep olmayacağından ayrıca TCK md. 244/1 gündeme gelmeyecektir.

İkinci olarak tezin hacking yöntemlerinin açıklandığı ikinci bölümünde aktarıldığı üzere, taşma/flooding saldırıları ya da benzer sonuçları doğuracak DoS/DDoS saldırıları sonucunda veri trafiğinin ağda düzgün işlemesini sağlayan protokolleri işleten sistemler bozulur ise verilerin taşma sonucunda ağdaki tüm sistemlere gönderilmesi söz konusu olacaktır. Örneğin ağdaki Ethernet protokolünün işleyişi bozulur ise X bilgisayarının Y bilgisayarına gönderdiği veriler Y bilgisayarı ile birlikte ağdaki sair sistemlere de gönderilir ve bu sayede fail ne X ne de Y sistemine erişmeden, bu trafiği izleyebilir. Böyle bir durumda TCK md. 243/4'ün yanında ayrıca TCK md. 244/1 de oluşacaktır.

4.2.1.5. İlliyet Bağı

Suçun objektif tipikliğinin oluşabilmesi için fiil ile netice arasında illiyet bağının varlığı şarttır. İlliyet bağına dair detaylı bilgi için yetkisiz erişim suçu yönünden yapılan açıklamalara bakılmalıdır. Araya girme suçu yönünden örnek vermek gerekirse, örneğin gönderici bilişim sistemi veya ağdaki switch üzerinde ağ iletişimine dair protokolleri işleten yapı düzgün çalışmaz ise X ile Y sistemi arasında iletilmesi gereken veriler, üçüncü taraf Z sistemine iletilebilir. Böyle bir durumda bu yanlış iletimde bir dahli olmayan kişi(*Z*) yönünden TCK md. 243/4 bağlamında gerçekleşen neticeye dair illiyet bağı oluşmayacaktır.

4.2.2. Sübjektif Tipiklik[488]

Suçun sübjektif tipikliğinin oluşumu için failde kast ve hukuka aykırılık bilincinin bulunması gerekir.[489] Suçun olası kastla işlenmesi mümkündür. Bir kişi verilerin kendisine iletilebileceğini öngörmesine ve bu durumun haksızlık doğuracağından şüphelenmesine rağmen neticeye kayıtsız kalarak, ''başka amaçlarla'' IP ve/veya MAC adresini değiştirir ya da istemci/gönderici sistemi veya veri iletim protokollerini işleten sistemleri bozarsa, neticeden olası kastla sorumluluğu doğacaktır.

[488] Yetkisiz erişim suçunun açıklandığı üçüncü bölümde anlatılan yapay zeka kullanımında sübjektif sorumluluğa dair sorunlar noktasında araya girme suçu yönünden önem arz eden bir husus bulunmadığından, bu konuda ilgili bölüme bakılmalıdır.

[489] Berrin AKBULUT 2017, age. s. 168; Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 910 / Hukuka aykırılık bilincinin gerekmediğine dair zıt yöndeki görüşler için bkz. Murat Volkan DÜLGER 2022, age. s. 296, 297, 298 vd.

Yine örneğin bahçeli evinin belirli noktalarına faraday kafesi etkisi yapacak şekilde tel çekmeyi isteyen ve bu amaçla evinin wi-fi veri trafiğinin hangi noktalara iletildiğini ve hangi mesafeden bu trafiğin izlenebileceğini hesaplamaya çalışan bir kişi, bu ölçümleri sırasında kendi trafiğini izlemeye çalışırken çevre evlerden gelen veri trafiğini de izlemiş olabilir. Eğer fail bu durumu öngörmesine rağmen neticeyi gerçekleştirmiştir ve haksızlık şüphesi içerisindedir denilebiliyor ise bu noktada failin olası kast ile TCK md. 243/4'ten sorumluluğu gündeme gelecektir.

4.3. SUÇUN HUKUKA AYKIRILIK UNSURU

4.3.1. Suç Tipi ile Bağdaşabilen Hukuka Uygunluk Sebepleri

Araya girme suçu yönünden TCK'da yer alan hukuka uygunluk sebeplerinden meşru savunma dışındakilerinin tatbiki mümkündür. Meşru savunmanın ise bu suç yönünden bir hukuka uygunluk sebebi olamayacağını düşünüyoruz. Yetkisiz erişim suçu yönünden meşru savunma tartışılabilir ise de araya girmenin haksız bir saldırıya yönelik savunmalarda kullanılmasına dair bir olayın gerçekleşmesi söz konusu olamayacağından, bu husus teorik tartışmalardan da bağımsız kalmaktadır. Böyle bir durum ancak ülke savunmasında istihbarat toplama noktasında dolaylı bir savunma durumu yaratabilir ki bu durum da zaten kanun hükmünü icra sebebiyle hukuka uygun olacağından, meşru savunma bir hukuka uygunluk sebebi olmayacaktır.

4.3.1.1. Hakkın Kullanılması

Araya girme suçu yönünden meşru bir hakkın kullanılmasının hukuka uygunluk sebebi teşkil etmesi, sözleşmeden doğan hakların kullanımı ve velayet hakkının kullanımı gibi durumlarda mümkündür. Ayrıca detayları yetkisiz erişim suçu noktasında açıklandığı üzere, işverenin bu yönde işçiyi bilgilendirmeden işçinin özel hayatı ya da özel haberleşmeleri ile ilgili olduğu açıkça anlaşılmayan verileri incelemesi mümkün olduğundan, işçinin işin gereği olarak yaptığı veri trafiğinin izlenmesi/dinlenmesi de bazı durumlarda hukuka uygun olacaktır. Evvela işverenin salt iş için kullanılması gereken iç ağda; ağ içi iletişimde ve iç ağdan WAN'a gönderilen/WAN'dan gelen verilerde veri paketlerinin içeriğine erişmeden, normal bir paket analiz yazılımı çalıştırarak ne tür bir veri trafiğinin gerçekleştirildiğine ve gönderici/alıcı bilgisine ulaşacak şekilde trafiği izlemesi meşrudur. Aşağıda açıklandığı üzere toplu kullanım sağlayıcı olan işverenler açısından trafiğe dair bu tür bilgilerin izlenerek kaydı zaten bir yükümlülüktür. Öyleyse bu noktada tartışılması

gereken esas konu, veri paketlerinin içeriğindeki bilgilerin de öğrenilmesini sağlayacak şekilde bir izlemenin tatbik edilip edilemeyeceğidir.

Kanaatimizce iş yerlerinde ağ içi iletişimde veri paketlerinin içeriğine erişebilecek yöntemler vasıtasıyla trafiğin izlenmesi meşru olabilir. Bunun için çalışanların ağ üzerinde sadece iş ile ilgili iletişimleri gerçekleştirmeleri gerektiğinin bilincinde olmaları şarttır. Zira ancak bu halde çalışanların ‘’*veri trafiğinin gizliliğine dair bir meşru beklentileri*‘’ bulunmayacaktır. İç ağ ile WAN iletişiminde ise eğer iletişimin WAN'daki tarafı da çalışan değilse veya veri trafiğinin gizliliğine dair meşru bir beklenti içerisindeyse, bu kişinin rızası alınmadan veri paketlerinin içeriğine erişilebilecek şekilde bir izleme tatbik edilemez. Böyle bir durumda veri trafiğine dair bilgiler de rızaya aykırı olarak ‘’hakkın kullanılması‘’ kapsamında öğrenilemeyecek olmakla birlikte, belirtildiği üzere toplu kullanım sağlayıcılar açısından trafiğe dair genel bilgilerin izlenmesi ile kaydı normatif bir yükümlülüktür.

Belirtmek gerekir ki bu suç yönünden sistemler üzerindeki mülkiyet yahut zilyetlikten kaynaklanan hakların bir hukuka uygunluk sebebi teşkil etmesi mümkün değildir. Zira bir kimse salt maliki olduğu için başka birine verdiği sistem üzerinden yapılan trafiği araya girerek izleyemez. Bu noktada ayni haklardan ayrı olarak, mutlaka işçi-işveren ilişkisine dayalı haklara ya da toplu kullanım sağlayıcılara getirilen yükümlülüklere benzer bir yasal dayanağa sahip olunması gerekir.

4.3.1.2. Kanun Hükmünü İcra

4.3.1.2.1. Veri Trafiğinin İzlenmesi ve Dar Manadaki Trafik Bilgisinin Kaydedilmesi Yükümlülüğü

İnternet hukuku mevzuatımızda erişim sağlayıcıların, yer sağlayıcıların ve toplu kullanım sağlayıcıların internet trafiğine dair bir kısım logları tutma yükümlülüğü bulunmaktadır. Mevzuatta trafik bilgisi olarak adlandırılan bu loglar, zaman damgasıyla hash fonksiyonu kullanılarak saklamakta ve bu sayede adli bilişim faaliyetlerinin başarıya ulaşabilmesi ile faillerin ve delillerin tespiti amaçlanmaktadır. Yer sağlayıcılar veri trafiğinin istemci ve/veya sunucu tarafında olduklarından, nakil halindeki verilerin göndericisi veya alıcısı konumunda bu logları kaydederler. Bir bilişim sisteminin kendisinin nihai alıcı/gönderici olduğu durumda karşı taraftan gelen trafiğe dair verileri kaydetmesi ise TCK md. 243/4'e konu fiili oluşturmayacağından, bu yükümlülükler araya girme suçu nazarında değerlendirilemez.

Erişim sağlayıcılar ise istemci-sunucu arasındaki veri trafiğini, işlettiği internet omurgası üzerinde kurduğu sistemler ya da trafiği kendi kontrolündeki proxy sunucular üzerinden geçiriyor ise trafiği bu sunucular vasıtasıyla mitm konumunda izlemekte ve iletişimin tarafı olmadığı halde gönderici ile alıcı tarafa dair trafik bilgilerini izlemekte/kaydetmektedir. Toplu kullanım sağlayıcılar da kendi ağlarına bağlı olan üçüncü tarafların kullanımındaki bilişim sistemleri ile aynı ağdaki veya sair bir ağdaki başka bir sistem arasındaki iletişimde, kontrolü altındaki router/modem/switch/proxy ve mitm konumundaki sair bir sistem üzerinden trafiği izler ve kaydeder. Erişim sağlayıcıların ve toplu kullanım sağlayıcıların iletişimin tarafı olan sistemlere erişmeden gerçekleştirdiği bu izleme işlemi TCK md. 243/4'ün objektif tipikliği içerisinde kalmasına rağmen, bu yöndeki normatif yükümlülükleri icra ediyor olmaları sebebiyle bu durum hukuka uygun olacaktır.

Erişim sağlayıcılar yönünden hukuka uygunluk sebebini teşkil eden ve yükümlülük getiren normlar; 5651 s. Kanun md. 6, Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği md. 19/1-f, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik md. 8 ve Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik md. 15'te yer alan düzenlemelerdir. Toplu kullanım sağlayıcılar yönünden ise bu normlar; 5651 s. Kanun md. 7 ve İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik md. 4 ile 5'te yer almaktadır.

Erişim sağlayıcıların ve toplu kullanım sağlayıcıların nakil halindeki verileri iletişimin tarafı olan bilişim sistemlerine erişmeden teknik araçlar vasıtasıyla izlemesinin yukarıdaki normlar gereğince hukuka uygun sayılabilmesi için bu izleme faaliyetlerinin ancak ve ancak ilgili normlarda zikredilen, ''dar manadaki trafik bilgisini'' açığa çıkartacak şekilde olması şarttır. Öyle ki bu normlara dayanılarak DPI kullanımı veya proxy sunucular üzerinde çalıştırılan yazılımlar sonucu normatif sınırların ötesinde bilgilere ve örneğin iletişimin içeriğine dair bilgiye erişilebilecek yöntemlerle trafiğin izlenmesi durumunda, TCK md. 243/4'e konu fiil ve netice meydana gelecektir.

Bu konuya dair diğer bir önemli husus, erişim sağlayıcılara yükümlülük getiren iki temel kanunun mevcudiyetidir. Bunlardan ilki, erişim sağlayıcıların elektronik haberleşme sektörüne dair faaliyetleri gereğince sahip olduğu hak ve yükümlülüklere dair düzenlemeleri barındıran Elektronik Haberleşme Kanunu'dur. İkincisi ise adli

bilişim, siber güvenlik ve erişimin engellenmesine dair kararlar yönünden yükümlülükler getiren 5651 s. Kanun'dur. Her iki kanuna bağlı yönetmeliklerde de erişim sağlayıcılara trafiği izleme ve bu dar manadaki trafik bilgisini kaydetme yükümlülüğü getirilmiş olup, bu duruma bağlı olarak erişim sağlayıcılar hem elektronik haberleşme sektörüne dair faaliyetleri ve hem de bundan ayrı olarak adli bilişim ile siber güvenlik gereğince dar manadaki trafik bilgisine yönelik veri trafiğini izler ve kaydeder. Genel olarak elektronik haberleşme sektörüne dair faaliyetler gereğince tutulması gereken trafik bilgileri ile adli bilişim/siber güvenlik gereğince tutulması gereken trafik bilgilerinin kapsamı neredeyse aynı olduğundan, izlemeye dair farklı teknikler kullanılması gerekmez. Lakin yine de trafiğe dair verilerin izlenmesinin hukuka uygun olabilmesi için iki yükümlülük alanının birbirine karıştırılmaması ve bir alandaki dayanak norma göre diğer alana yönelik bir uğraşa girişilmemesi gerekir.

4.3.1.2.1.1. Yükümlülüğün Kapsamında Kalan Dar Manadaki Trafik Bilgisi

Mevzuatımızda trafiğe dair bazı bilgi türleri normatif olarak ''trafik bilgisi'' şeklinde isimlendirilmektedir. Veri trafiğine dair her türlü bilgi, özünde trafik bilgisi olduğundan, mevzuatta sıralanan bu bilgi türlerinin ''dar manadaki trafik bilgisi'' şeklinde nitelendirilmesi daha doğru olacaktır.

4.3.1.2.1.1.1. Erişim Sağlayıcılar Yönünden

Veri trafiğine dair genel bilgileri kapsayan ''dar manadaki trafik bilgisi'' kavramı, siber güvenlik ve adli bilişime dair yükümlülükler getiren 5651 s. Kanun'da ''*taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri*'' şeklinde tanımlanmıştır. 5651 s. Kanun'un uygulama yönetmeliği olan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik md. 3/1-ö'de ise proxy sunucu trafik bilgisi, erişim sağlayıcıların kontrolündeki proxy sunucular yönünden

> ''*internet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi gibi bilgileri*''

şeklinde tanımlanmıştır. Dayanak kanunu 5651 s. Kanun olan bir diğer yönetmelik olan Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara

Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik md. 3'te ise erişim sağlayıcı trafik bilgisi,

> ''*İnternet ortamına erişime ilişkin olarak abonenin adı, adı ve soyadı, adresi, telefon numarası, abone başlangıç tarihi, abone iptal tarihi, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri*''

şeklinde tanımlanmıştır. Elektronik haberleşme hizmetinin sunumu ve sektörel yükümlülüklerin yer aldığı Elektronik Haberleşme Kanunu'na dayanılarak yürürlüğe konulmuş olan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunmasına İlişkin Yönetmelik md. 4'te ise trafik bilgisi ''*Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veri*'' şeklinde tanımlanmıştır. Aynı kanuna dayanılarak çıkartılan Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği md. 19/1-f'de ise aynı kavram ve kavrama dair yükümlülüğe yönelik

> "*Erişim sağlayıcı olan veya telefon hizmeti sunan işletmeci, taraflara ilişkin IP adresi, port aralığı, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı, kullanıcı sayısı ve abone kimlik bilgileri ile altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini iki yıl süreyle; kullanıcı bilgilerini ise ilgili mevzuatta belirtilen zamanaşımı süresi boyunca muhafaza etmekle yükümlüdür.*''

şeklinde bir düzenlemeye gidilmiştir.

Erişim sağlayıcıların trafiğe dair tutmakla yükümlü olduğu bu trafik bilgisi kayıtları, ilgili normlarda birbirinden farklı saymalara tabi tutulmuş ve tahdidi olarak da sayılmamıştır. Bu normlardan, veri paketlerinin katmanlarının içeriğine erişilmemesi ve verilerin içerdiği hiçbir bilginin bu izlemeler vasıtasıyla elde edilmemesi gerektiği yönünde somut bir olgu açıkça ortaya çıkmaktadır. Öyle ki bu normlar ile verilerin içeriğine değil, veri trafiğine dair genel bilgilerin öğrenilmesi istenmektedir. Bu bilgiler de normlarda sayılan; sistemlere dair adres/kimlik bilgisi olan IP-port-MAC bilgisi, gönderilen verinin boyutu-gönderim ve alım tarihi, kullanılan protokoller, işletim sistemi ile uygulamalar, komut bilgisi ve trafikteki verilere dair benzer genel nitelikli bilgilerdir. Her ne kadar normlarda abone kimlik ve adres bilgileri de trafik bilgileri arasında sayılsa da bunlar veri trafiğinin izlenmesi sonucu değil, erişim sağlayıcının IP-abone eşleştirmesi yapması sonucunda, elinde bulunan abone verilerinden hangisinin trafiğe dair olduğunu ortaya koyması ile gerçekleşir.

Yukarıda zikredilen normlarda yer alan düzenlemelerde sınırlı bir sayma yapılmaması, trafiğe dair normlarda sayılanların ötesindeki bilgilerin de elde edilip edilemeyeceği noktasında bir hukukilik sorunu yaratabilir. TCK md. 243/4 bağlamında bu normların yaratabileceği ikinci sorun ise hedef sisteme dair bilgiler yönündendir. Yetkilendirme Yönetmeliği'nde genel olarak, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'te ise yalnızca trafiği proxy üzerinden geçiren erişim sağlayıcılar yönünden, hedef sisteme yani iletişimin alıcı tarafına dair trafik bilgisinin de izlenmesi ve kaydı yükümlülüğü getirilmiştir. Diğer normlarda ise trafiği proxy üzerinden geçirmeyen erişim sağlayıcılara dair trafik bilgileri tanımlanırken, muğlak bir ifade ile ''*ilgili bağlantı için verilen IP adresi*'' şeklinde bir tanımlama yapılmıştır. IP adresini veren/atayan erişim sağlayıcı bu işlemi abonesine yönelik yaptığından, burada iletişimin alıcı tarafı eğer erişim sağlayıcının işletmediği farklı bir omurga üzerinde bulunuyor ya da aynı omurga üzerinde bulunmakla birlikte farklı bir erişim sağlayıcıdan abonelik hizmeti alıyor ise bu durumda istemci-sunucu ikilisine IP atayan erişim sağlayıcılar birbirinden farklı olacaktır. Öyleyse normlardaki ''*ilgili bağlantı için verilen IP adresi*'' düzenlemesini hedef sistem bilgisi şeklinde anlamak mümkün görünmemektedir. Bu sebeple dayanak normda açıkça zikredilmiyorsa, hedef sisteme dair IP-port ve sair bilgileri açığa çıkartacak şekilde veri trafiğinin izlenmesinin TCK md. 243/4 nazarında hukuka uygunluğu sorunludur.

4.3.1.2.1.1.2. Toplu Kullanım Sağlayıcılar Yönünden

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik md. 3/1-e'de ''erişim kayıtları'' şeklinde adlandırılmış olan dar manadaki trafik bilgisi,

> ''*Kendi iç ağlarında dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş zamanını ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri, hedef IP adresi, bir veya birden fazla IP adresinin portlar aracılığı ile kullanıcılara paylaştırılması yöntemi ile sunulan internet erişim hizmetinde kullanıcıya tahsis edilen gerçek IP ve port bilgileri*''

şeklinde tanımlanmıştır. Erişim sağlayıcıların kaydetmesi gereken trafik bilgilerine dair yapılan tahdidi olmayan saymaların aksine, toplu kullanım sağlayıcılar yönünden son derece açık bir düzenlemeye gidilmiştir. Öyleyse toplu kullanım sağlayıcıların iletişimin tarafı olan bilişim sistemlerine erişmeden veri trafiğini kanun hükmünü icra kapsamında izlemeleri için ancak bu bilgilere erişebilecek şekilde sınırlandırılmış bir teknoloji kullanmaları gerekir.

4.3.1.2.2. İletişimin Tespiti Kararları

Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile TİB'in Kuruluşuna Dair Yönetmelik md. 3/1-i'de

> ''*İletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemler*''

şeklinde tanımlanan iletişimin tespiti, bilişim sistemlerinin iletişim kurduğu internet ve sair ağ teknolojileri nazarında yukarıda açıklanan dar manadaki trafik bilgilerinin tespitine verilen bir diğer isimdir. Her türlü elektronik haberleşme teknolojisi vasıtasıyla yapılan iletişimlere dair erişim sağlayıcılarda ve sair servis sağlayıcıda veya doğrudan bu iş için kurulan merkezlerde önceden kaydedilmiş durumda bulunan verilerin, ceza yargılamalarında yahut istihbarat faaliyetlerinde bilgi elde etme amacıyla muhatabından celbine yönelik normatif dayanaklar mevzuatımızda mevcuttur. Bu normlar; TCK md. 135, PVSK ek md. 7, MİT Kanunu md. 6[490] ve JTGYK ek md. 5 düzenlemeleridir. Bu hükümlere dayanarak verilen kararlar geçmişte yapılan iletişimlere dair kayıtlı bilgileri konu edindiği takdirde, bunun TCK md. 243/4 bağlamında bir önemi olmayacaktır. Lakin bir soruşturma sırasında yahut istihbari amaçlar doğrultusunda geleceğe yönelik iletişimin tespiti yapılacak ise ilgili normlar, veri nakillerinin izlenmesi yönünden TCK md. 243/4 nazarında bir hukuka uygunluk sebebi teşkil edecektir.

4.3.1.2.3. İletişimin Dinlenmesi Kararları

TCK md. 243/4 yönünden hukuka uygunluk sebepleri nazarında en çok önemsenmesi gereken husus, iletişimin tespiti ile aynı normlarda dayanak bulan ''iletişimin dinlenmesi'' kararlarıdır. Geleceğe yönelik telekomünikasyon yoluyla yapılan iletişimin mecburen teknik araçlarla dinlenmesine/izlenmesine cevaz veren bu normlar, iki bilişim sistemi arasında yapılan iletişimin bu sistemlere erişmeden

---

[490] Kanunda hem üçüncü kişi vatandaşların hem yabancıların ve hem de özel olarak MİT ile ilişkili kişilerin dinlenmesine/izlenmesine dair düzenlemeler mevcuttur. Bkz. md. 6'nın ilgili kısmı: ''*... telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. ... Önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuranların iletişimi tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. ...*''

dinlenmesi/izlenmesi yönünden bir hukuka uygunluk sebebi teşkil edecektir. PVSK ek md. 7'de

> ''*Bu maddede belirtilen telekomünikasyon yoluyla yapılan iletişime ilişkin işlemler ile 5271 sayılı Kanunun 135'inci maddesi kapsamında yapılacak dinlemeler, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde tek bir merkezden yürütülür*.''

denilmiş, MİT Kanunu'nda da aynı düzenlemeye gidilmiş, Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile TİB'in Kuruluşuna Dair Yönetmelik hükümlerinde de bu faaliyetlerin BTK nezdinde kurulacak merkezden yürütüleceği belirtilmiştir. Lakin BTK'nın iletişimin dinlenilmesine/izlenmesine yönelik konumu doğrudan bilişim sistemleri aracılığıyla yapılan trafiği izlemek olabileceği gibi buna yönelik teknik altyapısı yok ise özellikle internet iletişiminde gündeme gelebileceği üzere bu yönde erişim sağlayıcılar ile işbirliği yaparak dinleme/izlemeyi gerçekleştirmesi de mümkündür.[491] Örneğin CMK md. 137'de erişim sağlayıcıların bu yöndeki kararların gereğini yapacağı açıkça zikredilmiştir. Buna ek olarak Elektronik Haberleşme Kanunu md. 12/2-g'de erişim sağlayıcıların yasal dinleme ve müdahalelere imkan sağlamak zorunda olduklarına dair bir düzenleme de mevcuttur. Öyleyse BTK nezdinde veya erişim sağlayıcılar üzerinden yapılacak izlemelerde, izlemeyi kimin yaptığı ve hangi norma dayalı olarak izlemenin yapıldığına dair değişiklik gösterebilecek şartlar mevcut olduğu zaman, ilgili görevliler yönünden bu normlar TCK md. 243/4 bağlamında bir hukuka uygunluk sebebi teşkil edecektir.[492]

Bu düzenlemelerin internet iletişimi ve benzer ağ teknolojileri ile yapılan iletişimlere konu veri trafiğinin izlenmesi noktasında TCK md. 243/4 bağlamında bir hukuka uygunluk sebebi olacağı söylenebiliyor ise de ''dinleme kararının özü'' gereği veri paketlerinin içerdiği bilgilere(*örn. konuşmalara*) erişildiği için bu bilgiler elde edilmeye çalışılırken sair bir kısım suçların oluşması mümkündür. Zira GSM ve benzeri altyapı üzerinden gerçekleştirilen telefon görüşmelerinin aksine internet teknolojisi ve benzeri ağ yapılarındaki iletişimlerde, yakalanan verilerin analizi sonrası paket içeriklerine sınırsız bir erişim kolay değildir. İletişimi derinlemesine dinlenmek/izlenmek istenen sistemlere erişilmeden bu işlemi gerçekleştirebilmek için

[491] Bu normlar internet iletişimi dahil her türlü telekomünikasyon altyapısı vasıtasıyla yapılan iletişimler yönünden işlevseldir. Benzer yönde bkz. Mustafa TAŞKIN 2011, age. s. 83, 84, 85, 90, 200 vd.; Yasin SÖYLER 2013. age. s. 145; Cumhur ŞAHİN 2019, age. s. 355; Hakan KARAKEHYA 2016, age. s. 355; Murat BALCI, M.Emin ALŞAHİN ve Kerim ÇAKIR 2021, age. s. 500; Dijital Ceza Muhakemesi Hukuku, s. 513.

[492] Benzer yönde bkz. Murat Volkan DÜLGER 2022, age. s. 326, 327.

mevcut olan seçeneklerden biri; erişim sağlayıcılar ile omurga üzerinden ya da bu yönde kurulan bir merkezden, derin paket analizi(*DPI*) yapacak teknolojileri kurarak, veri paketlerinin içeriğine erişmektir. Böyle bir durumda eğer sadece belirli uygulama yazılımları ve protokollerin işletilmesi vasıtasıyla gerçekleştirilen trafiğin yakalanıp paket içeriklerinin analizi teknolojik olarak başarılamıyorsa(*bu tür yazılımlar mevcuttur*), dinleme kararının amacına aykırı olarak trafiği dinlenen/izlenen kişinin yaptığı bütün internet iletişimi izlemeye takılacaktır. Örneğin şüphelinin Whatsapp, mail ya da Skype iletişimine konu olabilecek haberleşmelerin izlenmesi, dinleme kararları yönünden amaca dair etkili bir araçtır. Lakin sınırlama yapılamadığında, alakasız biçimde elektronik bankacılık işlemleri, elektronik ticaret sitelerinden yaptığı alışverişleri ve hatta Google aramaları dahil ziyaret edilen bağlantılara dair veri trafiği de izlenecektir ki bu durum dinleme kararlarının amacı ile bağdaşmayacaktır. Aynı şekilde veri trafiği genellikle kriptolandığı için bilgilere ulaşılabilmesi ve dinleme/izlemenin yapılabilmesi için kriptonun da cebren kırılması gerektiğinden, bu cebri müdahalelere yönelik hukuki dayanak sorunları mevcut olacaktır.[493]

4.3.1.2.4. MİT Kanunu'nda Yer Alan Özel Düzenlemeler

İletişimin dinlenmesine dair normlarda genel olarak somut bir olay bulunur ve kararın hukukiliği hakim onayına bağlanır. Ancak MİT Kanunu md. 6'da genel bir ön alan araştırması niteliğinde, daimi bir izleme faaliyeti gerçekleştirilmesi mümkün kılınmıştır.

> ''*Önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuranların iletişimi tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir*.''

şeklindeki düzenlemeye göre yetkilinin onayı ile belirli bir süreye ya da olaya göre sınırlandırılmamış bir elektronik haberleşme takibi gerçekleştirilebilecektir.

Bu hüküm gereğince MİT'in ilgili görevlilerinin bilişim sistemlerine erişmeksizin veri trafiğini teknik araçlar ile izlemesi, TCK md. 243/4 nazarında kanun hükmünü icra hukuka uygunluk sebebi gereğince meşru olacaktır. Örneğin bu yönde elektromanyetik dalgalar ile aktarılan verilerin yakalanıp analiz edilmesi için büyüklü

[493] Bu konuda detaylı yorumlar için bkz. Alp ÖZTEKİN 2021, age. s. 195, 196, 197.

küçüklü alıcı sistemlerinin çeşitli coğrafyalara kurulması ve çalıştırılması mümkündür. Yine yakalanan veri paketlerinin tüm katmanlarının detaylı analizi için spesifik yazılımlar geliştirilmesi ve kullanılması da bu düzenleme sınırında yapıldığı sürece mümkün görünmektedir.

4.3.1.3. Rıza

Rızanın TCK md. 243/4 yönünden bir hukuka uygunluk sebebi teşkil etmesi mümkündür. İletişim ve veri nakilleri tek taraflı olamayacağından, bu suç yönünden tek taraflı verilen rıza yalnızca trafiğe yönelik rızayı veren istemcinin bilgilerinin izlenilmesini hukuka uygun kılabilir. Trafiğe dair hedef sisteme yönelik bilgilerin elde edilebilmesi için iletişimin diğer tarafının da rızasının bulunması yani çoklu rızanın mevcudiyeti şarttır. Bu suçun korumayı amaçladığı değerler bilişim sistemleri üzerindeki mülkiyet hakkı veya yetki veren sair bir hak olmadığından, rızayı veren tek kişinin iletişimdeki tüm sistemlerin maliki olması da rızayı geçerli kılmayacaktır. Örneğin bir kişi kendi üzerine kayıtlı iki akıllı cep telefonundan birini eşine ve diğerini de çocuğuna vermiş olabilir. Bu kişinin rızası sonucu üçüncü bir kişinin, eşi ile çocuğu arasındaki Whatsapp görüşmelerine dair veri trafiğinin izlenmesi mümkün değildir. Aynı şekilde bu kişinin rızası ile üçüncü bir kişinin, kendisi ile eşi ya da çocuğu arasındaki mail trafiğine dair verileri izlemesi de karşı tarafın rızası alınmadığında hukuka aykırı olacaktır. Bu noktada internet iletişimine yönelik toplu kullanım sağlayıcıların dar manadaki trafik bilgilerine dair izleme/kayıt yükümlülüğünün ayrık bir hukuka uygunluk sebebi yaratacağı ise unutulmamalıdır.

Rıza noktasında TCK md. 243/4'e yönelik verilebilecek somut bir örnek, bir kimsenin ağ bağlantısını üçüncü taraflara kullandırtıyor ve karşılığında ''*veri nakillerinin izlenmesine rıza gösteriyorum*'' şeklinde bir rıza beyanı alıyor olmasıdır. Böyle bir durumda internet iletişimi yönünden birden fazla kişiye sistemlerini kullandıran kişinin konumu toplu kullanım sağlayıcı olacağından ve izlemeler dar manadaki trafik bilgileri yönünden kanun hükmünü icra gereğince hukuka uygun olacağından, rıza noktasında tartışılması gereken temel konu, dar manadaki trafik bilgilerinin ötesindeki bilgilere yönelik izleme faaliyetleri yahut kişinin toplu kullanım sağlayıcı sayılmadığı ihtimallerdir. Yukarıda zikredildiği üzere bu ihtimallerde iletişimin salt tek tarafının rızası ile diğer taraflara yönelik trafik bilgileri elde edilemez. İnternet trafiğinde ise iletişimin karşı tarafları önceden belirli olmadığından, rızaları alınabilecek somut kişiler söz konusu değildir. Öyleyse pratikte gönderici-alıcı

arasındaki veri trafiğinin izlenmesi ve bu sayede gönderici-alıcı sistemlere yönelik bilgilere ulaşılabilmesinin rıza sonucu hukuka uygun olabilmesi ancak internet trafiğine kapalı CAN ve/veya LAN ağlarında yapılan ağ içi iletişimlerde ve tüm tarafların bu izlemeye dair rızası bulunduğu durumlarda mümkün olacaktır.

Rıza noktasında diğer bir önemli husus ise veri trafiğinin hangi derecede izlenmesine rıza gösterildiği hususudur. Açıktır ki rızanın salt trafiğe dair bilginin öğrenimine yönelik verildiğinde, bu rızaya dayanarak verilerin içerdiği bilgilerin öğrenimine yönelik bir izleme faaliyeti tatbik edilemez. Ancak veri paketlerini yakalayan yazılımların/cihazların her biri aynı sayı ve nitelikte paketleri yakalayacak ve aynı sınırlarda analiz gerçekleştirecek diye bir kural olmadığından, trafiğe dair bilgiler noktasında rızanın her bir bilgi tipi yönünden açıkça verilmesi gerektiği dile getirilebilir. Lakin bir kişi ‘’*ağ üzerinden gerçekleştirilen iletişimlerde trafik bilgilerimin izlenmesine rızam vardır*‘’ şeklinde bir beyanda bulunulur ise asgari olarak dar manadaki trafik bilgilerine dair normlarda sayılan bilgi tipleri yönünden rızanın geçerliliği kabul edilmelidir.

4.4. SUÇUN KINANABİLİRLİK UNSURU (*Kusurluluk*)

Araya girme suçunda kınanabilirlik yönünden önem arz eden pek bir husus yoktur. Bu noktada değinilmesi gereken tek mesele, kişilerin başka suretle elde edilemeyeceğini düşündükleri delilleri elde etmek amacıyla bilişim sistemleri arasındaki veri nakillerini, sistemlere erişmeksizin teknik araçlarla izlemesidir. Her olayın kendi özelinde değerlendirilmesi gerekiyor ise de böyle bir durumda zorunluluk halinin mevcudiyeti sebebiyle[494] suçun kınanabilirlik unsuru oluşmayabilir. Kınanabilirlik alt başlığı altında değerlendirilmesi gereken diğer bir konu olan suçun kınanabilirlik unsurunu kaldıran bir hataya düşülmesi haline yönelik görüşler için yetkisiz erişim suçunun kınanabilirlik unsuruna dair yapılan açıklamalara bakılmalıdır.

[494] Hamide ZAFER 2010, age. s. 111.

BÖLÜM V

SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ

5.1. TEŞEBBÜS

5.1.1. Yetkisiz Erişim Suçu Yönünden Suça Teşebbüs

Doktrindeki ağırlıklı görüş, yetkisiz erişim suçuna teşebbüsün mümkün olduğu yönündedir.[495] Doktrinde teşebbüs yönünden sisteme erişmek için şifrelerin kırılmaya çalışılmasına rağmen kırılamaması,[496] tam sisteme erişilecekken elektriklerin kesilmesi,[497] siber güvenlik uygulamalarının aşılmaya çalışılmasına rağmen aşılamaması ve hedef sisteme erişim yetkisi verecek malware yazılımların enjeksiyonu lakin çalıştırılamaması[498] şeklinde örnekler verilmektedir.[499] Suça kalmaya devam etme seçimlik hareketi yönünden teşebbüsün mümkün olmadığına dair görüşler mevcut olduğu gibi[500] bunun mümkün olduğu, kalmaya devam etmeye çalışılmasına rağmen sistemde kalınamamasının bu sonucu doğuracağı yönünde de görüşler mevcuttur.[501]

[495] Hasan GERÇEKER 2020, age. s. 2155; Doğan SOYASLAN 2020b, age. s. 664; Berrin AKBULUT 2017, age. s. 150; Burak ÇEKİÇ 2006, age. 94.
[496] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 242.
[497] Ali PARLAR ve Muzaffer HATİPOĞLU 2010, age. s. 3745.
[498] Cengiz APAYDIN 2017, age. s. 58; Büşra ÖZÇELİK 2019, age. s. 112.
[499] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 905, 906.
[500] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 242; Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 965; Berrin AKBULUT 2017, age. s. 151.
[501] Ali İhsan ERDAĞ 2010, age. s. 283.

TCK md. 35'e göre fail suça konu neticeyi gerçekleştirmeyi isteyerek(*kast*) ve bu neticeyi gerçekleştirmeye elverişli eylemleri ile suçun icrasına başladığında, suça konu netice elinde olmayan nedenlerden dolayı oluşmaz yani suç tamamlanamaz ise teşebbüsten dolayı sorumlu tutulacaktır. Yetkisiz erişim suçu, neticesi harekete bitişik bir suçtur ve sisteme erişim durumunun meydana gelmesi ile suçun objektif tipikliği oluşacaktır. Bu sebeple teşebbüse konu fiiller sisteme erişmek/kalmaya devam etmek değil, sisteme erişmeye/kalmaya devam etmeye çalışmaya dair eylemlerdir.[502] Bu tür eylemlerin ise ancak hazırlık hareketleri haricinde kalanları suça teşebbüs nazarında bir sorumluluk doğurabilecektir.

Doktrindeki genel eğilimin de bu yönde olduğu üzere yetkisiz erişimin ''sisteme erişmek/girmek'' seçimlik hareketiyle işlenmesi yönünden suça teşebbüsün mümkün olduğu açıktır. Kanımızca kalmaya devam etme seçimlik hareketi ile suçun işlenmesi yönünden de suça teşebbüs mümkün olup, yetkili olarak erişimin gerçekleştirebildiği süreyi uzatmaya veya yetkisi bittiği an sistem ile bağlantısını kesecek olan yazılımı devre dışı bırakmaya çalışan biri bunu başaramaz ve hareketleri de suçun işlenmesine elverişli olur ise teşebbüsten söz edilebilir. TCK md. 243/3'te düzenlenen yetkisiz erişim suçunun neticesi sebebiyle ağırlaşmış haline ise kast+taksir kombinasyonu gerektiğinden, teşebbüs mümkün değildir.[503]

Yetkisiz erişim suçu yönünden teşebbüs noktasında önem arz eden ilk husus, neticeyi gerçekleştirmeye yönelen eylemlerin hazırlık hareketi olmaması gerektiğidir. Örneğin bir malware yazılımın kişinin kendi sisteminde suç işlemeye yönelik hazırlık gereğince tutuluyor olması teşebbüse konu edilemez. Lakin ''*sistemdeki verilere ulaşma ve/veya sistem içeriğine kontrol altında bir müdahale imkanı*'' yazılımın çalışır vaziyette olması ile doğuyorsa, yazılımın çalıştırılamaması veya düzgün çalışmayarak bu imkanları sağlamaması durumunda suça teşebbüs gerçekleşecektir.[504]

Bir diğer önemli husus ise hazırlık hareketi olmayan ve neticeyi gerçekleştirmeye yönelen eylemlerin, suçun işlenmesine elverişli olmasının gereğidir. Özellikle yetkisiz erişim suçu yönünden eylemlerin neticeyi gerçekleştirmeye elverişli

[502] Suç tipini salt hareket suçu olarak gören lakin bu noktada benzer yöndeki görüşler için bkz. Berrin AKBULUT 2017, age. s. 150.
[503] Berrin AKBULUT 2017, age. s. 151; Yargıtay 5. CD 2008/13177 E. 2008/9607 K. İçinde, Tan, age. 735.
[504] Fatih Selami MAHMUTOĞLU 2013, age. s. 861; Ahu Karakurt EREN 2020, age. s. 753; Cengiz APAYDIN 2017, age. s. 58; Büşra ÖZÇELİK 2019, age. s. 112.

olması, çeşitli hacking yöntemleri açısından üzerinde ciddiyetle durulması gereken bir husustur. Zira brute force saldırılarının ya da URL üzerinden gönderilen http istekleri veya çeşitli vasıtalarla gönderilen SQL komutlarının gönderiminin çok basit şekillerde yapılması mümkündür. Eğer bir kişinin web platformu kullanıcı adı xxx ve şifresi de 000 ise alelade bir denemede herhangi bir kişinin bu sisteme yetkisiz erişimi mümkün olacaktır. Aynı şekilde ekstrem derecede istek filtreleme açıkları bulunan bir sunucuda, alan adından sonra rastgele girdiler yazılması sonucunda, sunucudaki dosya isimleri ile komutlara dair kodlamaların bu rastgele girdiler ile eşleşerek sistemlere yetkisiz şekilde erişilmesi gündeme gelebilir. Bu şekilde rastgele bir SQL açığından yararlanılması da ihtimal dahilindedir. Öyleyse herhangi bir şifre girişine 000 yazılması ya da tarayıcının URL girişine rastgele girdiler girilip istek yollanması ve hatta bu durumların defalarca tekrarlanması gibi durumlar mecburen suçun icrasına elverişli hareketler olarak kabul edilecektir.[505]

5.1.2. Araya Girme Suçu Yönünden Suça Teşebbüs

TCK md. 243/4'te düzenlenen araya girme suçuna teşebbüs teoride mümkündür.[506] Lakin pratikte böyle bir durum ancak istisnai durumlarda yaşanabilir. Zira kablolar içerisinde ya da elektromanyetik dalgalar vasıtasıyla akan veri trafiğinde, bu nakil halindeki veri paketlerini gerekli teknolojiyi kullanan herkes yakalayabilmektedir. Suç veri trafiğine dair bilgilere erişmeyi konu edinmediğinden; kriptolanmış olsun ya da olmasın salt veri paketlerinin yakalanması suça konu fiil ve neticeyi oluşturacak, veri paketlerinin yakalanması ise havadan bir veriyi alıp sepete koymak gibi somut bir işlem olmadığı ve gönderici-alıcı arasındaki iletişime müdahale de edilmediğinden, kullanılan teknolojiler düzgün çalıştığı an suçun objektif tipikliği oluşacaktır. Bu tür teknolojileri bulundurmak hazırlık hareketi, bu tür teknolojileri kullanmadan trafiği izlemeye çalışmak ise suça elverişsiz bir hareket olacaktır. Öyleyse kanaatimizce TCK md. 243/4'e teşebbüsün mümkün olabileceği tek ihtimal, kullanılan teknolojinin düzgün çalışmamış ve paketleri yakalayamamış olmasıdır.[507]

[505] Aksi yönde görüşler için bkz Büşra ÖZÇELİK 2019, age. s. 113.
[506] Aynı yönde bkz. Berrin AKBULUT 2017, age. s. 168. Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 911.
[507] Berrin AKBULUT 2017, age. s. 168.

5.2. İŞTİRAK

TCK'nın 37 ila 41. maddelerinde düzenlenen iştirak hükümlerine göre iştirakçiler, suça dair gerçekleştirdikleri katkıya göre müşterek fail, dolaylı fail, azmettiren ve yardım eden olarak suçtan sorumlu tutulurlar. Hem yetkisiz erişim hem de araya girme suçları yönünden; yetkisiz erişim suçunun neticesi sebebiyle ağırlaşmış haline iştirak ve BT çalışanlarının durumu haricinde, iştirak hükümlerinin uygulanabilirliği noktasında işbu tez kapsamında tartışılması ya da ortaya konulması gereken herhangi bir husus bulunmamaktadır.[508]

Neticesi sebebiyle ağırlaşmış suçlarda kast + taksir kombinasyonu bulunduğundan, direkt olarak ağırlaşan neticeye ve neticesi sebebiyle ağırlaşmış suçun işlenmesine dair bir iştirak iradesi söz konusu olamaz. Ancak neticesi sebebiyle ağırlaşmış suçlarda da iştirak hükümlerinin uygulanması mümkün olduğundan,[509] TCK md. 243/3 yönünden suça iştirak söz konusu olabilecektir. İştirakçilerin neticesi sebebiyle ağırlaşmış suçtan iştirak hükümlerine göre sorumlu tutulabilmeleri için ağırlaşan neticenin, failler arasında suçun işlenmesine dair mevcut olan ortak iradenin sınırları içerisinde kalması gerekir.[510] Örneğin suç ortağı bir çalışan, iç ağda kritik verilerin tutulduğu sunucuya erişebilecek MAC adresine sahip bilgisayarına diğer suç ortağının uzaktan bağlantı kurması için rootkit yazılımları kurabilir. Ağ dışındaki suç ortağı da rootkit üzerinden ortağının bilgisayarına bağlanır ve oradan da kritik verilerin tutulduğu sunucuya brute force saldırıları başlatarak, yetkisiz olarak erişir. Bu olayda ağ dışındaki suç ortağı trafiğini gizleyeceği ve hatta köle bilgisayar kullanabileceği için tespiti zor olacak, ağ içerisindeki suç ortağı da rootkitler kendini gizleyeceğinden ve geçmiş işlem bilgisini silebileceğinden sanki hacklenmiş ve suçun işlenmesinde dahli yokmuş izlenimi yaratacaktır. İşte böyle bir olayda brute force saldırıları sırasında bir şekilde istenmeden sunucu bozulur ve veriler silinir ise TCK md. 243/3'te düzenlenen suç oluşacaktır. Suç ortaklarının iradesi brute force saldırısı yönünden birleştiğinden, ağ içerisindeki iştirakçi yönünden neticesi sebebiyle ağırlaşmış suçta müşterek fail sıfatı doğacaktır. Lakin bu kişiler farklı bir olayda aynı binaya hırsızlık yapmak için girseler ve biri kapıyı gözlerken diğeri açık bilgisayarı fark edip kendi iradesi ile birtakım işlemler gerçekleştirdikten sonra istemeden verilerin silinmesine sebep olsa, bu işlemler yönünden ortak bir irade bulunmadığından, kapıyı gözleyen iştirakçinin

[508] Benzer yorumlama için bkz. Hasan GERÇEKER 2020, age. s. 2155.
[509] Yargıtay 1. CD 2008/6619 E. İçinde, Koray DOĞAN 2015, age. s. 284.
[510] Nevzat TOROSLU ve Haluk TOROSLU 2021, age. s. 352.

TCK md. 243/3 yönünden iştirak hükümlerine göre bir sorumluluğu doğmayacaktır. Doktrinde ayrıca haklı olarak, neticesi sebebiyle ağırlaşmış suçlardan iştirakçilerin sorumlu tutulabilmesi için ağırlaşan neticeyi sübjektif olarak öngörme imkanına sahip olmaları gerektiği de belirtilmektedir.[511]

Yetkisiz erişim ve araya girme suçları yönünden BT çalışanlarının da iştirakçi olması gündeme gelebilir. Örneğin en temel siber güvenlik uygulamalarından olan firewall sistemlerinde, gelen-giden istekler yönünden engellenecek olan IP-Port-MAC-alan adı-URL ve sair kombinasyonlara dair beyaz/siyah listeler bulunur.[512] Eğer WAN'dan sınırlı erişim yapılması isteniyor ve kapalı bir ağ yapısı ya da intranet platformu oluşturulacak ise genellikle yalnızca izin verilen bağlantıların yer alacağı listelerde, izin verilenler harici bağlantılar külliyen engellenir. Bu tür bir sınırlama bulunmuyorsa, standart firewall sistemlerinin asgari düzeyde ülkelerdeki düzenleyici ve denetleyici kurumlar yahut sair resmi kurumların yayınladığı[513] veya bu yöndeki uluslararası dokümanlarda yer alan zararlı bağlantılara dair gelen-giden istekleri engellemesi gerekir.

Bir BT çalışanı yetkisini kötüye kullanarak firewall ayarlarını değiştirebilir ve sisteme veri gönderememesi gereken bir bağlantı ile veri alış verişine izin vererek, bunun sonucunda da sisteme malware gönderimi ve sair şekillerde ataklar gerçekleştirildikten sonra yetkisiz erişim neticesinin doğmasına sebep olabilir. Böyle bir durumda hacker ile BT çalışanının suçun işlenmesine dair ortak bir iradesi bulunuyor ise iştirak yönünden bir sorun doğmayacak, BT çalışanı da hacker da iştirak halinde yetkisiz erişim suçundan sorumlu tutulacak, BT çalışanı yardım eden konumunda suça iştirak etmiş sayılacaktır.

BT çalışanlarının asıl failler ile ortak bir iştirak iradesine sahip olmadığı durumlarda, çalışanların kasten ihmal ettiği/kaldırdığı siber güvenlik önlemlerinin yetkisiz erişim suçunun işlenmesini kolaylaştırması noktasında iştirak hükümlerinin uygulanabilirliği de tartışılması gereken bir meseledir. Doktrinde TCK md. 244 yönünden, BT çalışanlarının/teknik elemanların ihmali hareketler ile kasten siber güvenlik önlemlerini almamaları durumunda suçun faili olabilecekleri zikredilmektedir.[514] Esasında yazılımlar güncellenmediği zaman güvenlik açıkları

[511] Koray DOĞAN 2015, age. s. 281.
[512] Teemu VAİSANEN, Lorena TRİNBERG ve Nikolas PİSSANİDİS 2016, age. s. 49.
[513] Ülkemiz yönünden bu kurum BTK ve bünyesindeki USOM'dur.
[514] Murat Volkan DÜLGER 2022, age. s. 339.

oluşabileceği gibi sistem odası gerektiği gibi temizlenmediğinde dahi bilişim sistemlerinde bozulmalar gerçekleşebilir[515] ve bu durumlar da yetkisiz erişim yapılmasında yardımcı unsur olabilir. Böyle bir durumda sistem odasını kasten temizlemediği için siber güvenlik uygulamalarını barındıran sunucuların arızalanmasına ve bu sebeple ağda güvenlik açıklarının oluşmasına sebep olan temizlikçinin ya da pisliği görmesine rağmen önlem almayan sistem odası görevlisinin TCK md. 244 yönünden iştirak halinde sorumlu olabilecekleri açık ise de aynı sonuca işlenmesini kolaylaştırdıkları yetkisiz erişim suçu yönünden ulaşmak bu kadar kolay değildir.

Gerek sistemlerin bozulmasını sağlayarak gerekse siber güvenlik önlemlerini almayarak veya devre dışı bırakarak kasten sistemlerde güvenlik açıkları yaratan kişiler, sistemlerin/platformların şifrelerini başkaları ile paylaşan kişiler veya yetkisiz erişim suçlarının işlenmesini kolaylaştıracak sair eylemleri gerçekleştiren kişiler yönünden TCK md. 243/1 açısından iştirak halinde sorumluluğun doğumu, iştirak iradesinin varlığına bağlıdır. Her ne kadar iştirakçiler arasında ortak bir anlaşma yapılmış olmasına ve hatta iştirakçilerin birbirlerinden haberdar olmasına dahi gerek bulunmasa da iştirak halinde sorumluluk için işlenecek veya işlenmekte olan somut bir suça bilerek katkı sağlamak şarttır ve bu da iştirak iradesini teşkil eder.[516] Öyleyse sırf işverenini sevmediği için kasten siber güvenlik açıkları oluşturan bir çalışan, sisteme kuvvetle muhtemel yetkisiz erişimde bulunulacağını düşünmüşse, sisteme daimi olarak bu tür saldırılar gerçekleştirilmekteyse veya yapılacak somut bir saldırıdan haberdar olduktan sonra bu güvenlik açığını yaratmışsa, TCK md. 243/1'den yardım eden sıfatıyla iştirak halinde sorumlu olacaktır.

Doktrinde yetkisiz erişim suçuna iştirak yönünden bu suçun işlenmesine yardım etmek için bilişim sistemini veren kişinin iştirak halinde sorumlu olacağı örneği verilmektedir. Şüphesiz ki bu örnek araya girme suçu yönünden de geçerlidir.[517] Yine örneğin bir kişinin komşusunun wi-fi veri trafiğini izlemek için bu işlerden anlayan bir tanıdığını azmettirerek evine çağırması ve birlikte komşusunun veri trafiğini izlemeleri durumunda da iştirak halinde TCK md. 243/4'ün işlenmesi söz konusu olacaktır.

[515] Gökhan USTA 2018, age. s. 23.
[516] Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 780, 781, 784.
[517] Ramazan DOĞAN 2014, age. s. 95.

5.3. İÇTİMA

5.3.1. Suçun Zincirleme Şekilde İşlenmesi

5.3.1.1. Aynı Mağdura Karşı Suçun Aynı İcra Kararı Çerçevesinde Zincirleme Şekilde İşlenmesi

Yetkisiz erişim veya araya girme suçlarının zincirleme biçimde işlenmesinin ilk şekli, TCK md. 43/1'de yer alan düzenleme gereğince, aynı suç işleme kararının icrası kapsamında bu suçun aynı mağdura karşı birden fazla kere işlenmesi durumudur. Bu durumda hareket ve neticenin çokluğuna bağlı olarak çok sayıda cezaya değil, ağırlaştırılmış tek bir cezaya hükmolunur.

Aynı suç işleme kararının icrası sırasında, tek bir sisteme birden çok kere yetkisiz erişim gerçekleştirilmesi veya aynı sistemlere dair veri trafiğinin izlenmesi durumlarında zincirleme suç hükümlerinin uygulanması gerektiği açıktır.[518] Ancak TCK md. 43/1 yönünden tez konusu suçlar için önemsenmesi gereken ilk mesele, zincirleme suçun oluşumu için sistemin değil mağdurun aynı olmasının yeterli olacağıdır. Bu sebeple failin aynı mağdurun yetkisi altında bulunan pek çok sisteme aynı suç işleme kararının icrası sırasında ayrı ayrı erişmesi veya benzer durumun araya girme suçu yönünden oluşması durumunda da zincirleme suç hükümleri uygulanacaktır.[519] Bu durumun pratikte tecelli etme olasılığı da oldukça kuvvetlidir. Örneğin bir hacker ağ yapısına brute force saldırısı yaparak yetkisiz olarak eriştiğinde, bu yetkisiz erişim neticesine ek olarak ağdaki sair sistemlere de erişmesi kuvvetle muhtemel olduğundan, ağdaki sistemler tek bir yetkiliye sahip ise TCK md. 43/1 uygulanacaktır.

Belirtmek gerekir ki sistemlerin sanallaştırılmış bölümleri ayrı bilişim sistemleri olarak kabul edileceğinden, sanallaştırılmış her bir birime ve sanal birimleri içerisinde bulunduran fiziki sisteme yapılan erişimler farklı fiiller ve farklı yetkisiz erişim suçları doğuracaktır. İçerisinde farklı sanal birimler bulunan bir bilişim sistemi içerisindeki tüm bu ayrık alanlara ayrı ayrı yetkisiz olarak erişilir ise eğer suçlar tek bir suç işleme kararının icrası sırasında ve değişik zamanlarda işleniyor ve her bir sanal makine aynı mağdurun yetkisi altında bulunuyor ise bu noktada da TCK md. 43/1'in uygulanması gerekir.

---

[518] Murat Volkan DÜLGER 2022, age. s. 310, 311; Ankara Bölge Adliye Mahkemesi 8.CD 2017/207 E. 2018/439 K. İçinde, Uğur İHTİYAROĞLU 2020, age. s. 432, 433; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 248; Doğan SOYASLAN 2020b, age. s. 665.
[519] Ahmet Caner YENİDÜNYA 2005, age. s. 12.

TCK md. 43/1 yönünden tez konusu suçlar için irdelenmesi gereken bir diğer mesele ise zincirleme suç için mevcut olması gerekli olan, aynı suç işleme kararının icrasıdır. Yargıtay bir kararında aynı uygulama yazılımına birden çok kere yetkisiz erişilmiş olmasını zincirleme suç için yeterli görmüş,[520] sair bir kararında aynı web veri tabanına dört ayrı yetkisiz erişim gerçekleştirilmesi ve her seferinde farklı bir ders notunun veri tabanı üzerinden değiştirilmesi durumunda da zincirleme suç hükümlerinin uygulanması gerektiğine karar vermiştir.[521] Doktrinde ise uzun aralıklarla her seferinde farklı verilere erişilmesi için sisteme yetkisiz olarak erişim sağlanıyor ise zincirleme suç hükümlerinin uygulanmaması gerektiği belirtilmektedir.[522]

Failde bulunması gereken aynı suç işleme kararının icrası noktasında verilebilecek somut bir örnek, failin eski eşini sanal olarak takip etmek amacıyla kendisine arka kapılar yaratan rootkit yazılımlar kurduğu bir sisteme bu yazılımlar vasıtasıyla bir çok kere yetkisiz olarak erişmesidir. Bu örnekte rootkit yazılımlar çalıştığı sürece erişim devam edecek, rootkit yüklü sistem her kapatıldığında erişim kesilecek, tekrardan çalıştırıldığında ise erişim yenilenecektir. Bu döngü rootkit sistemden kaldırılmadığı sürece devam edecektir. Bu örnekte fail rootkit vasıtasıyla yaptığı erişimleri eski eşini sanal olarak takip etmeye yönelik suç işleme iradesi kapsamında gerçekleştirdiği sürece, kanaatimizce TCK md. 43/1'in araya giren zaman aralıklarından bağımsız biçimde uygulanması gerekir. Aynı şekilde bu durumda

TCK md. 43/1'in yetkisiz erişimlerde farklı verilere erişilmiş yahut farklı işlemler gerçekleştirilmiş olması durumundan da bağımsız olarak değerlendirilmesi gerekmektedir. Zira rootkitler çok farklı işlemler gerçekleştirebileceğinden, keylogger özelliği gösterebileceği gibi botnet özelliği de gösterebilir ya da spyware şeklinde de kullanılabilirler. Sistemde çalıştırıldıkları süreler boyunca bu yazılımlar eski eşi sanal olarak takip etmeye yönelik çalıştığı sürece çok farklı işlemler gerçekleştirmiş, çok farklı verilere erişim sağlamış da olsalar, otomatik olarak gerçekleştirilen her bir işlem yönünden TCK md. 43/1'in uygulanması gerekir.

Failde aynı suç işleme kararının icrasına yönelik bir irade bulunmuyorsa, zincirleme suç hükümlerinin uygulanması mümkün olmayacaktır. Örneğin yukarıdaki

[520] Yargıtay 8. CD 2014/3984 E. 2014/13848 K.
[521] Yargıtay 8. CD 2012/33044 E. 2014/236 K. İçinde, Nevzat ÖZSOY (2019), ''Yargıtay Kararları Işığında Doğrudan Bilişim Suçları'', *Yaşar Hukuk Dergisi*, C. 1, S. 2, ss. 295-352, s. 308.
[522] Hüdaverdi UÇAR 2014, age. s. 57.

örnekteki failin eski eşi bir e-ticaret sitesi işletiyor ve fail de eski eşini sanal olarak takip etmek amacıyla onun Whatsapp ve arama kayıtlarını ya da galerideki resimlerini öğrenebilmek için sistemine yetkisiz erişimler gerçekleştiriyor olsun. Eğer fail bir müddet sonra yetkisiz erişimini kıskançlık ya da sanal takip değil, satmak için sistemdeki e-ticaret kişisel verilerini elde etmek amacıyla gerçekleştirir ise bu fiil ile kıskançlık nedeniyle gerçekleşen önceki fiillerin aynı suç işleme kararının icrası kapsamında gerçekleştirildiğini kabul etmek mümkün olmayacak ve ayrı ayrı cezalandırma yapılacaktır.

Belirtmek gerekir ki yetkisiz erişim suçu yönünden hafifletici sebep ve temel halin zincirleme suç yönünden bir arada bulunması durumunda, cezada artırım daha ağır ceza öngören birinci fıkra yani suçun temel hali üzerinden yapılacaktır.[523] Örneğin küçük çaplı bir müzik platformundaki müzikleri bedelsiz dinlemek isteyen bir kişi hem platformun bedeli karşılığı hizmete açılan web uygulaması üzerinden veri tabanına yetkisiz erişerek hafifletici sebebe dair neticeyi gerçekleştirir hem de sunucuların tutulduğu sistem odasına girerek direkt olarak sunucular üzerinden müzikleri USB'sine kopyalamak için fiziki sunuculara yetkisiz erişir ise ikinci eylemi olan TCK md. 243/1 üzerinden zincirleme suça dair artırılmış ceza tatbik edilecektir.

TCK md. 243/3'te düzenlenen, yetkisiz erişim suçunun neticesi sebebiyle ağırlaşmış hali yönünden de zincirleme suç hükümlerinin uygulanmasının mümkün olduğu belirtilmektedir.[524] Doktrinde bir görüşe göre ancak birden fazla kere ağırlaşmış neticenin doğumu durumunda neticesi sebebiyle ağırlaşmış suçlara yönelik zincirleme suç hükümlerinin uygulanması mümkün olacaktır. Bu görüşe göre örneğin ancak aynı suç işleme kararının icrası kapsamında birden çok kere yetkisiz erişim suçu işleniyor ve her seferinde de istemeden veriler yok ediliyor ise zincirleme suç hükümleri uygulanabilecektir.[525] Biz bu görüşe katılmıyoruz. Kanaatimizce aynı suç işleme kararı dahilinde pek çok yetkisiz erişim suçu işleniyor ve bunlardan bir kısmı suçun temel halini, bir kısmı neticesi sebebiyle ağırlaşmış halini teşkil ediyor olsa bile cezada adalet açısından iki ayrı suçtan ceza verilmemelidir. Bu durumda TCK md. 43'ün lafzında aksi yönde bir düzenleme olmadığı ve zaten nitelikli haller ile temel halin birlikte işlenmesinde aynı yöntem izlendiği için daha ağır cezayı gerektiren norm üzerinden zincirleme suç hükümlerinin uygulanması doğru olacaktır. Zira aksi görüş

[523] Yargıtay CGK 2012/13-1543 E. 2013/257 K.
[524] Berrin AKBULUT 2017, age. s. 152.
[525] Koray DOĞAN 2015, age. s. 293, 294.

benimsenir ise kişi aynı suç işleme kararı icrasında 4 kere sisteme yetkisiz erişse ve bunlardan ikisinde verilerin istemeden bozulmasına sebep olsa, hem suçun temel hali ve neticesi sebebiyle ağırlaşmış halinden ayrı ayrı cezalandırılacak ve hem de TCK md. 43/1 gereğince bu cezalar ayrı ayrı zincirleme suç hükümlerine göre artırılacaktır. Cezalandırma noktasında normların sanık aleyhine bu denli ağır bir yoruma tabi tutularak tatbiki ise hakkaniyetli bir ceza hukuku felsefesi ile bağdaşamaz.

5.3.1.2. Aynı Fiil ile Birden Fazla Mağdura Karşı Aynı Suçun İşlenmesi

TCK md. 43/2'ye göre aynı suçun birden fazla mağdura karşı tek bir fiil ile işlenmesi durumunda da zincirleme suç hükümleri uygulanacaktır. Zincirleme suça dair bu durumun yetkisiz erişim ve araya girme[526] suçları yönünden oluşması, çoğu hacking eylemi yönünden kuvvetle muhtemeldir. Aşağıda farklı örnek olaylar üzerinden zincirleme suç hükümlerinin uygulanıp uygulanamayacağı üzerine değerlendirmeler yapılmıştır.

5.3.1.2.1. Yetkisiz Erişim Suçu Yönünden Örnek Durumlar

5.3.1.2.1.1. Aynı Fiil ile Birden Fazla Mağdura Ait Birden Fazla Bilişim Sistemine Yetkisiz Olarak Erişilmesi

Tek bir fiil ile birden fazla bilişim sistemine yetkisiz olarak erişilmesi, evvela içeriği sanallaştırılmamış birden fazla mağdura ait birden fazla bilişim sistemleri yönünden gündeme gelebilir. Örneğin bir web sitesine, çalıştırıldığı zaman sisteme erişim veya hakimiyet yetkisini sağlayacak türde bir malware içeren dosya yüklendiğinde, bu dosyayı ne kadar çok kişi indirirse indirirsin TCK md. 43/2 gereğince zincirleme suç hükümleri uygulanacak ve tek bir ağırlaştırılmış ceza verilecektir. Bu noktada ikinci örnek durum, P2P hosting sistemine dayalı uygulamalar yönündendir. Örneğin internet üzerinden erişilebilen bir X web uygulaması içerisindeki verileri pek çok farklı hostun kendi sunucusunda/bilgisayarında/sisteminde barındırması mümkündür. Herhangi bir içeriğe erişilebilmesi için yetkili olmanın şart koşulduğu ve örneğin şifre ya da sair bir soft token kullanımının gerektiği bu P2P uygulamaya yetkisiz olarak erişen fail, verileri barındıran her bir bilişim sisteminin sahibine/yetkilisine karşı tek fiili ile ayrı

[526] Berrin AKBULUT 2017, age. s. 169.

ayrı yetkisiz erişim suçları işlemiş olacaktır. Bu durumda da TCK md. 43/2 uygulanacak ve tek bir ağırlaştırılmış ceza verilecektir.

Tek bir fiil ile birden fazla bilişim sistemine yetkisiz olarak erişilmesi, ikinci olarak içeriği birden fazla mağdurun yetkisine tahsis edilmiş biçimde sanallaştırılmış olan donanımların varlığı durumunda gündeme gelebilir. Tek bir fiziksel bütünlüğe sahip sistemler içerisindeki sanallaştırılmış bölümlerin ayrı bilişim sistemleri sayılması gerektiğinden, bu durumda da tek bir fiil ile birden fazla mağdura karşı yetkisiz erişim suçunun işlenmesi gündeme gelecektir. Sanallaştırma uygulamalarında sanal birimler arasında geçiş güvenlik uygulamaları ile engellenir. Fakat sunucunun bütününe karşı gerçekleştirilen saldırılardan her bir sanal birimin etkilenmesi mümkündür.[527] Daha çok 244. maddedeki sistem engelleme/bozma suçu nazarında sonuçlar doğuracak bu durumun, sunucuya yapılan fiziki yetkisiz erişimler sonucunda birden fazla sanal birime tek fiil ile erişilmesi başarılabiliyor ise TCK md. 243 yönünden de gündeme geleceği açıktır. Ağ üzerinden tek fiil ile birden çok sanal birime yetkisiz olarak erişilmesinin ise sanallaştırma teknolojilerinin yarattığı sonuçlardan dolayı mümkün olmadığını düşünüyoruz.

5.3.1.2.1.2. Aynı Fiil ile Bir Bilişim Sisteminin Farklı Kişilerin Yetkisine Tahsis Edilmiş Alanlarına Yetkisiz Olarak Erişilmesi

TCK md. 43/2 yönünden tek fiil ile bir bilişim sisteminin farklı kişilerin yetkisine tahsis edilmiş alanlarına erişilmesi durumuna dair örneklerin anlaşılabilmesi için evvela iki hususun bilinmesi gerekmektedir. İlk olarak, bir bilişim sistemine yetkisiz olarak erişmek fiili, erişim devam ettiği sürece gerçekleştirilen işlemler yönünden temadi eder ve örneğin bilgisayarın BIOS'una, işletim sisteminin açılış bölümüne, kullanıcı ara yüzüne, kullanıcı ara yüzündeki bir klasöre, klasör üzerindeki bir uygulama yazılımına ve yazılım içerisindeki bir veriye erişim durumları ile erişim süresince gerçekleştirilen sair işlemler tek bir yetkisiz erişim fiilinin icrası kapsamında kalacaktır. Bilinmesi gereken ikinci husus ise donanım + siber uzaydan oluşan tek bir bilişim sisteminde, siber uzayın çeşitli kısımlarına erişime dair yetkinin farklı kişilere yahut birden fazla kişiye ait olabileceğidir. Bir fiziki sunucunun farklı sanal birimleri farklı bilişim sistemleri olarak kabul edildiği ve ayrı mağdurlara tahsisli bu sanal

[527] Işıl KARABEY AKSAKALLI, ''Bulut Bilişimde Güvenlik Zafiyetleri, Tehditler ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi'', *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, C. 5, S. 1, ss. 8-34, s. 12, 13, 14 vd.

birimlere tek bir fiil ile yetkisiz olarak erişilmesinin pek olanaklı olmadığı yukarıda zikredilmişti. Bu sebeple aşağıdaki açıklamalar yetkisiz olarak erişilen tek bir sistemin, farklı kişilerin yetkisinde olan alanlarına dair yapılmaktadır.

TCK md. 43/2 yönünden gündeme gelmesi muhtemel en temel olaylar, hosting hizmetine tahsis edilmiş web sunuculara yetkisiz olarak erişilmesidir. Örneğin bir web sunucunun mülkiyeti X şirketine, donanım + veri boyutuyla bunu kullanma hakkı aracı hosting firması Y'ye, sunucuda sitesine dair verileri depolama ve bu verilere erişme/değişiklik yapma hakkı ise hosting hizmeti alan müşteri Z'ye ait olabilir. Örnekte X şirketi sunucuları kendi veri merkezinde barındırmakta, işletim sistemine dair genel nitelikli işlemler ve genel güncellemeler ile sunucuların bakımını yapmakta, sunucu içerisindeki başkalarına tahsisli bölümlere ise sözleşme ilişkisinde belirtilen durumlar veya kanundan doğan zaruretler haricinde erişim hakkı bulunmamakta, sunucuya dair genel bir yetki sahibi durumunda bulunmaktadır. Aracı hosting firması Y ise web sitesi oluşturma, verileri barındırma, oluşturulan internet ortamlarına dair arka yüz-ara yüz veya sair uygulama yazılımlarını çalıştırma ve/veya SEO hizmetleri vermek için sunucunun veri boyutunu kendi müşterilerine tahsis etmiş(*alt kira gibi*), bu noktalara erişim ve müdahale hakkı ise müşterileri ile yaptığı sözleşmeler kapsamında sınırlandırılmıştır. Web sitesine dair tüm fikri mülkiyet, işletme hakkı ve içerisindeki verilere müdahale yetkisi ile bu müdahaleyi sağlayacak ara yüzü kullanma hakkı ise Y'nin müşterisi Z'de bulunmaktadır. Z ise kendi müşterilerine ait çok sayıda farklı kullanıcı ara yüzünün bulunduğu bir sosyal medya platformu işlettiğinden, her bir kullanıcı kendi ara yüzüne dair bir kısım veriler (*örn. fotoğraflar, yazışmalar*) üzerinde ayrıca yetkili konumdadır.

Suçun konusu temelde aynı ise bilişim sistemi iki ayrı kişiye ait olsa bile bu sisteme yetkisiz olarak erişildiğinde, iki ayrı mağdura karşı suç işlenmiş olmakla birlikte TCK md. 43/2 uygulanarak ceza artırılamaz.[528] Öyleyse TCK md. 43/2'nin uygulanabilmesi için aynı yetkisiz erişim fiili kapsamında erişilen siber uzay, veri dosyaları ve/veya çalıştırılan uygulamalara dair işlenmekte olan veriler farklı olmalıdır. Bu bakımdan, yukarıdaki örnekteki sunucuya ağ üzerinden yetkisiz olarak erişildiğinde eğer yetkisiz olarak erişilen alanda hem X hem Y hem de Z'nin hak ve yetkileri söz konusu ise TCK md. 43/2 uygulanmamalıdır. Zira böyle bir durumda sistemin yetkisiz olarak erişilen alanı aynı olacaktır. Lakin eğer yetkisiz olarak erişilen

[528] İzzet ÖZGENÇ 2021, age. s. 688, 689.

alan Z'nin müşterileri/sosyal medya platformu üyelerinin kullanıcı ara yüzlerine dair veriler ise Z ile üyelerin hak sahiplikleri aynı alana dair olsa bile üyelerin yetki sahibi oldukları alanlar kendi içerisinde farklı olduğundan, salt üyeler yönünden TCK md. 43/2'nin uygulanması gerekir. Zira böyle bir durumda tek fiil ile her biri farklı mağdurların yetkisine tahsisli farklı veri alanlarına yetkisiz olarak erişilmiş olacaktır.[529]

TCK md. 43/2 nazarında değerlendirilebilecek olayların web sunucular değil, bir bilgisayar veya benzeri sistemler yönünden gerçekleşmesi de mümkündür. Doktrinde bir bilişim sistemi içerisinde barındırılan verilerin hak sahibi ile bilişim sisteminin yetkilisinin farklı olması durumunda, yetkisiz erişim sonucunda üçüncü kişiye ait olan verilere de ulaşılması halinde TCK md. 43/2'nin gündeme geleceği belirtilmektedir.[530] Kanaatimizce bu yöndeki örneklerin veriler üzerindeki hak sahipliği değil, ''*farklı yetkililere tahsis edilmiş alanlar*'' üzerinden yapılması daha doğru olacaktır. Zira bu suçun korumayı amaçladığı değerler veriler üzerindeki haklar değil, bilişim sistemleri üzerindeki yetkili olma durumundan kaynaklı dokunulmazlıktır. Öyleyse bir sistemde tek bir yetkili bulunuyorsa, suçun mağduru tek olacağı gibi suçun konusu da tek olacak ve TCK md. 43/2'nin uygulanması mümkün olmayacaktır. Konuyu bir örnek ile somutlaştırmak gerekirse, örneğin bir kişi parasını ödeyerek indirdiği oyunları, bilgisayarında yeterli depolama alanı mevcut olmadığı için arkadaşının bilgisayarında barındırıyor olsun. TCK md. 43/2'nin uygulanabilmesi için bilgisayarın gömülü diski üzerinde barındırılan bu oyunların kullanım hakkının değil, ''oyunların barındırıldığı alana erişim yetkisinin'' yani esasında sisteminin kullanımı hakkının üçüncü kişinin yetkisine tabi kılınmış olması gerekir. Bu kişi oyunlarını arkadaşının bilgisayarında barındırıyor fakat barındırılan alana arkadaşının izni olmaksızın erişemiyor, oyunlarını oynamak istediğinde kendi USB cihazına aktarması ve tekrardan kendi bilgisayarına yükleyip çalıştırması gerekiyor ise oyunları barındıran sisteme yetkisiz olarak erişildiğinde sistem içerisindeki her bölüme erişim yetkisi sistemin tek sahibinde olacağından, TCK md. 243/1 yönünden tek mağdur sistemin sahibi olacak ve TCK md. 43/2 uygulanamayacaktır.

[529] Bu durumun pratikte tecelli edebilmesi için sunucuya fiziksel olarak erişilmesi ya da ağ üzerinden doğrudan Z'ye tahsisli sanal birime erişilmesi gerektiğini düşünüyoruz.
[530] Ahmet Caner YENİDÜNYA 2005, age. s. 12.

5.3.1.2.2. Araya Girme Suçu Yönünden Örnek Durumlar

Araya girme suçu, ‘’*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek*‘’ sonucu oluşur. Suçun objektif tipikliğinin oluşabilmesi için suçun konusu verinin nakil halinde olması, bir verinin nakil halinde olabilmesi için ise elektronik haberleşmenin tecellisi ve nihayetinde asgari bir adet gönderici ve bir adet de alıcının varlığı şarttır. Nasıl ki bir kişinin telefonu dinlendiği zaman haberleşmenin gizliliğini ihlal suçu yönünden konuşmanın tarafları mağdur sıfatını taşıyor[531] ise iki bilişim sistemi arasındaki VoIP telefon konuşmasına dair trafiğin izlenmesi durumunda da haberleşmenin tarafı kadar mağdur sayısı bulunacaktır. Haberleşmenin gizliliğini ihlal suçunda mektuplar yönünden PTT'nin ya da telefon konuşmaları yönünden GSM operatörünün mağdur sıfatına sahip olması gibi bir yorum yapılamadığı gibi araya girme suçu yönünden de erişim sağlayıcıların mağdur sıfatına sahip olması mümkün değildir.

İşte yukarıda zikredilen ve bu suçun doğasından kaynaklanan durum gereğince, araya girme suçunda çoğu zaman birden fazla mağdur bulunur. Lakin salt mağdur sayısı birden fazla diye TCK md. 43/2'nin bu suç yönünden direkt olarak uygulanması mümkün değildir. Öyleyse yetkisiz erişim suçu yönünden geçerli olan ‘’suçun konusunun farklı olması‘’ hususu, araya girme suçu yönünden daha fazla önem arz etmektedir. Araya girme suçu yönünden suçun konusunun farklı olabilmesi ve TCK md. 43/2'nin tatbiki için mecburen tek bir izleme fiili ile birden fazla farklı veri trafiğinin izlenmesi şarttır.

Belirtmek gerekir ki pratikte araya girme suçu yönünden TCK md. 43/2'nin ekseriyetle gündeme gelmesi mümkündür. Zira özellikle tek bir trafiği yakalaması için programlanmış bir teknoloji kullanılmıyorsa ve ağda sadece tek bir trafik akmıyorsa, herhangi bir ağdaki nakil halindeki veriler izlendiğinde, yakalanabilen tüm trafikler yakalanacak ve pek çok ayrı veri iletişimi izlenmiş olacaktır. Örneğin bir kişi oturduğu kafede wi-fi ağına dahil olup paket analiz yazılımını çalıştırdığında, ağdaki bütün trafiği izlemeye başlayacak ve kuvvetle muhtemel tek fiili ile birden fazla trafiği izleyecektir. Hatta bu kişi herhangi bir ağa dahil olmadan veri paketlerini yakalayabilen bir teknolojiyi çalıştırdığı zaman, sinyalleri kafeye ulaşan sokaktaki tüm kablosuz trafiği de izleyebilir.

---

[531] Damla KIZILARSLAN (2019), *Haberleşmenin Gizliliğini İhlal Suçları*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul, s. 79

Aynı şekilde ev LAN'ı ister kablolu ister kablosuz olsun, ağda kendisi dışında bir de kardeşinin bilgisayarının bağlı olduğu bir durumda kişi paket analiz yazılımını çalıştırdığı an kardeşinin birden fazla iletişimine dair veri paketlerini yakalamış ve örneğin hem X'e attığı maillerin ve hem de Facebook profili üzerinden gerçekleştirdiği işlemlerin veri nakillerini izlemeyi tek fiil ile başarmış olacaktır.

5.3.2. Bileşik Suç, Fikri İçtima, Geçit Suçu ve Gerçek İçtima

Yetkisiz erişim suçunun işlenmesine yönelik fiil salt bir sisteme erişim sağlamak, kalmaya bir saniye devam etmek, anında erişimi kesmek olmadığından ve erişim süresi boyunca yapılan işlemler de bu fiil içerisinde değerlendirileceğinden, suça konu fiil icra edilirken başka suçların objektif tipikliği içerisinde kalan neticelerin doğması muhtemeldir. Araya girme suçu yönünden de kısmen benzer bir durum mevcuttur. Örneğin banka hesabındaki parayı çalmak isteyen fail evvela internet bankacılığı portalına şifreyi kırarak yetkisiz erişecek ve bu sayede hem kişiler verileri ele geçirmiş hem de sisteme yetkisiz olarak erişmiş olacaktır. Failin erişim süresi içerisinde hesaptaki parayı başka yere aktarması hırsızlık, sistemdeki verilere müdahalesi ise verileri değiştirme suçunu teşkil edecektir. Fail şifreyi kırarken yasak cihaz ve programlar kapsamına dahil bir brute force yazılımını da pekala kullanılmış olabilir. İşte bu tür durumlarda suçların içtimaı yönünden pek çok değerlendirmenin bir arada yapılması gerekecektir. Aşağıda bu tür değerlendirmeler TCK md. 243 özelinde ve genel olarak birlikte işlenmesi muhtemel suçlar yönünden yapılmıştır.

Bu açıklamalardan önce TCK md. 243'ün TCK md. 245/A'da düzenlenen ''yasak cihaz veya programlar'' başlıklı suç normu ile ilişkisine değinmek doğru olacaktır. Bu suç yasak cihaz veya programların ''kullanılmasını'' objektif tipikliği içerisinde barındırmadığından, bir brute force saldırısında yazılım çalıştırılarak kullanıcı adı-şifre eşleştiğinde yazılımın otomatik olarak sisteme erişim gerçekleştirmesi söz konusu oluyor ise bu durumda fikri içtima ya da bileşik suç yönünden bir tartışma yapılmasına gerek yoktur. TCK md. 245/A'da bu tür bir yazılımın *imali, ithali, sevki, depolanması, kabulü, satışı, satışa arzı, satın alımı, başkalarına verilmesi veya bulundurulması* suç teşkil ettiğinden, yetkisiz erişimden ayrı bir fiil teşkil eden bu durumlarda daima gerçek içtima uygulanır.[532]

[532] Benzer görüşler için bkz. Ahu Karakurt EREN 2020, age. s. 242; Cengiz Apaydın (2020), ''Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu'', *Terazi Hukuk Dergisi*, C. 15, S. 163, ss. 563-571 s. 569; Berrin AKBULUT 2017, age. s. 170.

Konuya dair bir dipnot olarak eklemek gerekir ki tezin yetkisiz erişim suçunun unsurlarının aktarıldığı bölümde detaylı olarak zikredildiği üzere, yetkisiz erişim suçu(*243/2*) ile karşılıksız yararlanma suçu arasında özel-genel norm ilişkisi bulunmaktadır. Bu sebeple aynı fiil ile her iki suçun da birlikte oluşma olasılığı yoktur. Öyleyse karşılıksız yararlanma suçu yönünden suçların içtimaı/toplanması noktasında bir değerlendirme yapılmasına gerek bulunmamaktadır.

Nihai olarak yetkisiz erişim suçu ile araya girme suçunun kendi aralarındaki içtima durumuna da değinmek gerekir. Yetkisiz erişim suçu bir sisteme erişmeyi, araya girme suçu ise iletişimin gönderici-alıcı taraflarına ‘’erişmemeyi‘’ gerektirir. Bu sebeple aynı maddede düzenlenen tez konusu suçlar arasında içtima noktasında bir değerlendirme yapmaya gerek yoktur.

5.3.2.1. Yetkisiz Erişim Suçu

5.3.2.1.1. İçtima Yönünden Değerlendirme Yapılabilecek Suçlar

İçtima yönünden değerlendirme yapılabilecek suçların örnek bir olay üzerinden açıklanması daha sağlıklı olacaktır. Fail evden çalışan bir şirket yetkilisinin bilgisayarına sızmak için önce wi-fi bağlantı noktası ile bilgisayar arasındaki veri trafiğini izleyerek ağa dair şifreyi elde etmiş ve bu şekilde ağa dahil olmuş, bilahare de şirket intranetine erişim için gerekli şifreleri elde etmiştir. Hacker intranet sistemine istemci olarak eriştikten ve şirketteki sunucuya bağlandıktan sonra rootkit yazılımları sisteme enjekte eder ise bu sefer doğrudan yönetici olarak sunucuya erişmiş olacaktır. Bu şekilde yönetici yetkilerini elde eden hacker, sunucu içerisindeki çeşitli noktalara erişerek buradaki veri dosyalarının içeriğini öğrenebilir. Hacker önce sunucu içerisindeki ‘’müşteri kimlik bilgileri‘’ dosyasının içerisine erişerek kimlik bilgilerini öğrenmiş, ikinci olarak da mail kayıtlarının tutulduğu Outlook veri dosyasına erişmiş ve mail içeriklerini okumuştur. Maillerden birinde de çalışanın ‘’özel‘’ başlıklı maili ve içeriğinde de sevgilisi ile arasındaki evde çekilmiş özel fotoğraf çekimleri bulunmaktadır. Hacker sunucudan erişimini keseceği sırada delilleri karatmak ve/veya salt zarar vermek amacıyla root yetkisine dayanarak hem sistem geçmişini hem sistemdeki tüm klasörleri kalıcı olarak silmiştir. Aşağıdaki açıklamaların bir kısmı, içeriğinde içtima yönünden çeşitli ihtimalleri barındıran bu örnek olay üzerinden yapılmıştır.

5.3.2.1.1.1. Özel Hayatın Gizliliğini İhlal, Kişisel Verilerin Hukuka Aykırı Olarak Ele Geçirilmesi ve Haberleşmenin Gizliliğini İhlal Suçları

Yukarıdaki örnekte hacker yönetici yetkisiyle sunucuya yetkisiz olarak eriştiğinde evvela TCK md. 243/1'de düzenlenen yetkisiz erişim suçu meydana gelmiş ve suç erişim süresi boyunca işlenmeye devam etmiş olacaktır. Bu suçun işlenmesi sırasında müşteri kimlik bilgileri hukuka aykırı olarak ele geçirildiği için TCK md. 136, mail yazışmaları okunduğu ve haberleşmenin gizliliği ihlal edildiği için TCK md. 132 ve mail içerisinde bulunan özel hayata dair görüntülerin gizliliği ihlal edildiği için de TCK md. 134'te düzenlenen suçlar da oluşacaktır.[533]

Yetkisiz erişim suçunun unsurları veya nitelikli halleri arasında bu suçlara konu fiil ve neticeler yer almadığından veya tam tersi bir durum olmadığından, bu noktada TCK md. 42/1'in(*bileşik suç*) uygulanması mümkün olmayacaktır. Öyleyse bu durumda yetkisiz erişim fiili gerçekleştirildiği sırada meydana gelen ayrı ayrı suçlardan failin ne şekilde cezalandırılması gerektiği ehemmiyetle tartışılması gereken bir husustur.

Doktrinde bir görüşe göre başlıkta zikredilen suçların yetkisiz erişim suçuna konu fiil işlenirken oluşması durumunda, TCK md. 44'te ''*işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır*'' şeklindeki düzenleme gereğince, fikri içtima uygulanmalıdır.[534] Başka bir görüş ise yetkisiz olarak erişilen sistemde verilerin öğrenilmesi ile diğer suçların meydana gelmesi halinde araç suç-amaç suç ilişkisi kurulacağını ve araç suç ile amaç suçun icra hareketleri arasında bir örtüşme yoksa gerçek içtima gereği ayrı ayrı ceza verileceğini, aksi halde fikri içtimanın uygulanması gerektiğini belirtmektedir.[535] Kişisel verileri hukuka aykırı olarak ele geçirme yönünden durumu değerlendiren sair bir görüşe göre ise ''tüketen-tüketilen norm'' ilişkisi gereğince, yalnızca TCK md. 136'dan ceza verilmesi gerekir.[536] Kişisel verilere erişim yönünden bir değerlendirmede bulunan zıt yöndeki bir görüş ise kişisel verilerin ele geçirilmesi durumunda gerçek içtimanın uygulanacağını belirtmektedir.[537]

---

[533] Bu sonuçları doğuran sair örnekler için tezin işbu bölümünün ''5.3.2.1.2.1. Fikri İçtima'' başlığı altında yapılan açıklamalara bakılmalıdır.
[534] Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 966; Uğur İHTİYAROĞLU 2020, age. s. 432.
[535] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 906.
[536] Durmuş TEZCAN, Mustafa Ruhan ERDEM ve R. Murat ÖNOK 2021, age. 1161.
[537] Cengiz APAYDIN 2017, age. s. 95.

5.3.2.1.1.2. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu

Yukarıdaki örnekte hacker sisteme gerçekleştirdiği yetkisiz erişimini devam ettirirken TCK md. 243/1, bu erişimi sırasında sisteme rootkit yazılımlarını bilfiil yüklerken ve sistemdeki sair verileri silerken ise TCK md. 244/2'de düzenlenen suç oluşacaktır.[538]

Doktrinde bir kısım görüşler, sisteme erişmeden TCK md. 244'ün işlenemeyeceğini ve bu sebeple her daim yetkisiz erişim suçunun geçit suçu konumunda olacağını ve salt 244'ten ceza verilmesi gerektiğini belirtmektedir.[539] Benzer biçimde TCK md. 243'ün araç suç olarak işlenmesinin yaygın olduğu yönünde görüşler de mevcuttur.[540] İşbu tez kapsamında açıklanan hacking yöntemlerinde açıkça anlatıldığı üzere hedef sisteme erişmeden sistemler bozulabilmekte, veriler değiştirilebilmekte, silinebilmekte veya TCK md. 244'te zikredilen sair neticeler gerçekleştirilebilmektedir. Bu sebeple ilgili görüşler ile maddi gerçekler uyumlu olmadığından, meselenin teorik açıdan bu yönüyle tartışılmasına gerek bulunmamaktadır.

Doktrinde bir görüş, temel amacı sistemi engellemek olan bir fail bunu sisteme yetkisiz olarak erişerek gerçekleştirdiğinde fikri içtimanın uygulanması gerektiğini belirtmektedir.[541] Benzer şekilde TCK md. 243 ile 244 arasında fikri içtimanın uygulanması gerektiği yönünde görüşler mevcuttur.[542]

Doktrinde sair bir kısım görüşler ise salt md. 244 özelinde değil benzer durumlar yönünden de TCK md. 243 nazarında daimi bir araç suç/amaç suç ya da geçitli suç durumunun olmadığını lakin bazı durumlarda yetkisiz erişim haricindeki suça dair neticenin gerçekleştirilmesi için sisteme yetkisiz erişim gerekiyor ise bu durumda TCK md. 44'ün[543] veya geçit suçu teorisinin[544] tatbiki ile her iki suçtan değil, en ağır cezası olan suçtan ya da amaç suçtan cezalandırma yapılması gerektiğini belirtmektedir. Zıt yöndeki bir görüş ise TCK md. 244'teki suçun işlenmesi için sisteme erişilmesi her daim gerekli olmadığından, sisteme yetkisiz olarak erişildikten

---

[538] Hacker eğer normal verileri değil sürücü yazılımlarını silse idi sistem bozulacağından TCK md. 244/1 oluşacaktı.

[539] Şaban Cankat TAŞKIN 2008, age. s. 39; Ali PARLAR ve Muzaffer HATİPOĞLU 2010, age. s. 3745; Burak ÇEKİÇ 2006, age. s. 97; Cengiz APAYDIN 2017, age. s. 90, 91; Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ ve İlker TEPE 2021a, age. s. 966.

[540] Ali KARAGÜLMEZ 2014, age. s. 198.

[541] Yavuz ERDOĞAN 2010, age. s. 1419.

[542] Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 906.

[543] Berrin AKBULUT 2017, age. s. 152; İbrahim ŞAHBAZ 2020, age. s. 3131.

[544] Ali PARLAR ve Mustafa ÖZTÜRK 2020, age. s. 30; Nagihan GÜN 2020, age. s. 198. / Benzer yönde bkz. Doğan SOYASLAN 2020b, age. s. 665; Murat Volkan DÜLGER 2022, age. s. 314.

sonra TCK md. 244'e konu neticelere de kasten sebep olunması durumunda iki ayrı suçtan ceza verilmesi gerektiğini belirtmektedir. Bu yöndeki görüşlerden ilki normların korumayı amaçladığı değerlerin farklılığını gerekçe gösterirken,[545] diğeri burada iki ayrı hareketin iki ayrı neticeye sebep olduğunu ve bu sebeple iki ayrı suçtan ceza verilmesi gerektiğini belirtmektedir.[546]

Benzer durumlara dair Yargıtay ve istinaf mahkemeleri uygulamasında ise açıkça zikredilmese de sisteme yetkisiz erişimin TCK md. 244'ün bir unsuru olduğu düşünülerek(*bileşik suç*) ya da sisteme erişilmiş olduğu tamamen es geçilerek, ekseriyetle TCK md. 243 yönünden bir suçun oluşmayacağına karar verilmektedir. Örneğin,

> ''*... bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması, 2- Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince arttırılması gerektiğinin gözetilmemesi ...*''[547]

şeklindeki karardan açıkça üniversitenin veri tabanına yetkisiz olarak erişildiği ve sistemdeki notların/verilerin değiştirildiği görülmektedir. Lakin bir gerekçe belirtilmeden, sadece TCK md. 244'ün oluşacağı belirtilmiştir. Veri tabanına yetkisiz erişerek vergi ödemelerine dair verilerin değiştirilmesini konu eden bir kararda ise istinaf mahkemesinin TCK md. 244 ve devleti dolandırma suçlarından ayrı ayrı cezalandırma yapılması gerektiğine karar verdiği lakin yetkisiz erişime dair değerlendirme yapmadığı görülmektedir.[548]

Yargıtay,

> ''*Somut olayda; sanık ...'in, internet kafelerde bulunan veya bir şekilde temin ettiği bilgisayarlardan şikayetçiler ..., ..., ... ve katılan ...'in msn adreslerini kırarak, bu kişilere ait msn kişi listesinden belirlediği katılanlar ..., ..., ... ve mağdure ...'dan msn adreslerini kırdığı kişiler ile olan samimiyetlerine dayanarak bir yarışmada olduğundan ve kazanması için kontör göndermeleri gerektiğinden bahisle telefon kontörü istediği, bu şekilde elde ettiği kontör şifrelerini bilgisayar kafelerinde veya dışarda 3. şahıslara piyasa değerinin altında sattığı, sanık ...'ın da internet kafe*

[545] Emre İkbal AÇIKGÖZ 2017, age. s. 98.
[546] Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 269 / Ayrıca bkz. Olgun DEĞİRMENCİ 2019, age. s. 193.
[547] Yargıtay 8. CD 2012/33044 E. 2014/236 K.
[548] İstanbul Bölge Adliye Mahkemesi 13. CD 2017/1411 E. 2017/1483 K.

işlettiği ve sanık ...'den olan alacağını kontör bedellerinden mahsup ettiği, sanık ...'in bu şekilde nitelikli dolandırıcılık ***ve*** *bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçlarını, sanık ...'nin de sug eşyasının satin alınması veya kabul edilmesi suçunu işlediğine yönelik kabulde bir isabetsizlik görülmemiştir. ...*''[549]

şeklindeki bir uyuşmazlık yönünden ise pek çok farklı suç oluşmasına rağmen salt iki suç arasında gerçek içtima uygulayarak, *nitelikli dolandırıcılık ve bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme* suçlarından ceza verileceği yönünde karar kılmıştır. Halbuki olayda MSN şifresi kırılmış ve TCK md. 136 oluşmuş, kırılan şifre ile sisteme erişilmiş ve TCK md. 243/1 oluşmuş, erişilen sistem içerisinde veriler değiştirilerek yazışmalar yapılmış ve TCK md. 244/2 oluşmuş, yazışmalar ile dolandırıcılık da yapıldığından aynı zamanda TCK md. 158'e konu nitelikli dolandırıcılık suçu da oluşmuştur. Esasında bu olayda yazışmalar yapılarak sistemdeki verilerin değiştirilmesi ile dolandırıcılık suçları arasında açıkça fikri içtima durumu bulunmakta ve TCK md. 136 ile TCK md. 243 yönünden ayrı değerlendirmeler yapılması gerekmesine rağmen, fikri içtima da es geçilerek kanaatimizce hatalı bir sonuca ulaşılmıştır.

Yargıtay,

''*... 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, ...*''[550]

şeklindeki olayda da geçit suçu veya fikri içtimayı tartışmamış, doğrudan oluşan tek suçun TCK md. 244 olduğuna yani sanıyoruz ki bileşik suçun mevcudiyetine karar vermiştir.[551] Yargıtay, ilgili kısmı

''*… Somut olayda suç tarihinde ... Emniyet Müdürlüğünde Asayiş Şube Müdürü olarak görev yapan sanığın kendisine bağlı olan Aranan Şahıslar Büro Amirliğine gelerek atış eğitimine gitmek için bürodan ayrılmak üzere olan tanık ...'in kullandığı şahıs sorgulama sistemi açık olan bilgisayardan, tanık anlatımları ve bir bilişim sistemi olan ... kayıtlarına göre ... isimli şahsa ait silah ruhsatı almasına engel sicil*

[549] Yargıtay 15. CD 2014/19941 E. 2014/21437 K.
[550] Yargıtay 8. CD 2013/3173 E. 2014/18506 K.
[551] Ayrıca bkz. ''*Katılanın e-mail ve Facebook hesabına izinsiz girip hesapların şifrelerini değiştirmek suretiyle bilişim sistemine girmesini engellediğinden bahisle açılan davada; 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 suçlarında, gerçekleşen eylemlerin bir bütün olarak TCK.nun 244/2. mad- desinde düzenlenen suçu oluşturacağı ...* '' Yargıtay 8. CD 2015/1133 E. 2015/22729 K.

kaydını saat 15:24'te iptal ettiği, ... bilişim sistemine girilerek kaydın silinmesi sonucu ... isimli kişiye ... Kaymakamlığının 18.05.2009 tarihli olurları ile silah taşıma ruhsatı verilerek başkasına haksız bir çıkar sağlanması şeklindeki eylemin TCK.nun 244/2-son maddesindeki "bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme" suçunu oluşturduğu gözetilmeden, yazılı biçimde hüküm kurulması…''

şeklindeki benzer bir olayda da sisteme yetkisiz olarak erişildikten sonra sistemdeki verilerin değiştirilmesi sonucu haksız çıkar sağlanması noktasında sadece TCK md. 244'ten hüküm kurulması gerektiğine karar vermiştir.[552]

Yargıtay, ilgili kısmı

''*... bilirkişi raporunda;"Dominand Hukuk Yazılımları" isimli firma tarafından üretilen "Dominand Trafik Sorgu" isimli yazılımın bilgileri ve rızaları dışında kurum ile herhangi bir protokol ve sözleşme yapmadan veri tabanına izinsiz erişimin sağlandığı, firmanın bu yazılımı ücret karşılığı isteyen herkese aynı şifre ve kullanıcı adı ile sisteme giriş yapmak sureti ile sattığı, bundan maddi kazanç elde ettiği, www.dominandhukuk.com.tr isimli web sitesi üzerinden kişisel bilgileri hukuka aykırı olarak ele geçirerek yetkisiz kişilere yayılmasının sağlandığı, www.adresprogrami.com isimli web sitesinden ... isimli firma tarafından üretilmiş yazılım kullanılarak 50 milyon civarında kayıtlı kişinin nüfus bilgilerinden bazıları veya TC kimlik numarası ile sorgulama yaparak kişilerin adres ve nüfus bilgilerine ulaşılması ve mahrem bilgilerin yetkisiz kişilerin eline geçmesinin sağlandığı, bunun karşılığında maddi menfaat temin edildiği, adres rehberi uygulamasının adı geçen firma tarafından 1010 dolar artı KDV fiyatına satışının yapıldığı, ... sanıkların katılan kurumun bilişim sistemine girdikten sonra var olan verileri depoladıkları ve bu verileri satarak haksız menfaat elde ettiklerinin anlaşılması karşısında, eylemlerinin TCK'nın 244/3-4* ***ve*** *136/1 madde ve fıkrasında düzenlenen bilişim sistemlerinin işleyişini bozma ve kişisel verileri hukuka aykırı olarak ele geçirme suçlarını oluşturduğu gözetilmeden, suç vasfında yanılgıya düşülerek yazılı şekilde, TCK'nın 243/1 maddesi uyarınca mahkumiyet hükmü kurulması, Bozmayı gerektirmiş olup, ...*''

şeklindeki kararında ise kararın lafzında ''*veri tabanına izinsiz erişimin sağlandığı*'' belirtilmesine rağmen TCK md. 244 ve TCK md. 136'dan gerçek içtimaya göre ayrı ayrı ceza verilmesi gerektiğine karar vermiş lakin sanıyoruz ki yetkisiz erişimi TCK md. 244'ün bir unsuru olarak değerlendirdiğinden, TCK md. 243'ün oluşmadığına karar vermiştir.[553] Olayda kullanılan yazılım yönünden TCK md. 245/A'nın tartışılmamış olması da şüphesiz ki karardaki eksik yönlerdendir.

[552] Yargıtay 8. CD 2015/14782 E. 2016/4928 K.
[553] Yargıtay 15. CD 2017/15688 E. 2019/15288 K.

Uygulamada herhangi bir gerekçeye dayandırılmadan, bir kullanıcı ara yüzüne erişim/üyelik şifresinin bir şekilde elde edilmesi/kırılması, ardından şifre ile sisteme yetkisiz olarak erişilmesi ve bilahare şifrenin değiştirmesi durumları bir bütün olarak ‘’sistemdeki verileri erişilmez kılma‘’ şeklinde algılanmakta ve salt md. 244/2’den hüküm kurulmaktadır. Halbuki şifrenin öğrenilmesine dair TCK md. 136 ve yetkisiz erişim noktasında da TCK md. 243’ün de bu tür olaylarda değerlendirilmesi gerekir.

Örneğin ilgili kısmı,

‘’*… sanığın katılan ...'in e posta adresinin ve facebook hesabının şifresini kırması, ardından da şifreyi değiştirmesi şeklindeki eyleminden dolayı TCK'nın 244/2 maddesinde düzenlenen bilişim sistemindeki verileri bozma yoketme, erişilmez kılma, sisteme veri yerleştirme suçundan da mahkumiyet kararı verilmesi gerekirken yazılı şekilde hüküm kurulması …*‘’[554]

şeklindeki ve ilgili kısmı,

‘’*… Oluşa, katılanın aşamalardaki anlatımlarına, sanığın babasına ait internet hesabından katılana ait elektronik posta hesabına bir çok kez girildiğine ilişkin Microsoft ve TİB'den gelen yazı yanıtlarına ve tüm dosya kapsamına göre; katılana ait elektronik posta hesabının şifresini ele geçirerek bu adrese giren ve şifreyi değiştirmek suretiyle katılanın elektronik postalarına erişimini engelleyen sanığın, eylemine uyan TCK.nun 244/2. maddesi uyarınca cezalandırılmasına karar verilmesi gerekirken yazılı gerekçeyle beraat hükmü kurulması …*‘’[555]

şeklindeki ve yine ilgili kısmı,

‘’*… Yargıtay Ceza Genel Kurulu'nun 09.10.2007 gün ve 2007/11-44-200 sayılı kararında da açıklandığı üzere bilgisayar sistemine girilerek bazı sınav sonuçlarının değiştirilmesi şeklindeki eylemin 5237 sayılı TCK'nın 244. maddesindeki "*bilişim *suçunu" oluşturacağı …*‘’[556]

şeklindeki kararlar bu yönden eksiktir.

Yargıtay ilgili kısmı,

‘’*… Oluşa ve dosya kapsamına göre; sanık ...'ın, kız arkadaşı olan mağdur ... ile aralarındaki arkadaşlık ilişkisi sona erdikten sonra, mağdura ait facebook hesabının önceden bildiği internet şifresini, onun bilgisi ve rızası dışında değiştirerek, hakkı bulunmadığı halde giriş yaptığı mağdurun facebook hesabında, beraber oldukları dönemde mağdurun bilgisi dahilinde kaydettiği cinsel içerikli görüntülerini*

[554] Yargıtay 15 CD 2017/31912 E. 2018/2652 K.
[555] Yargıtay 8. CD 2012/31216 E. 2013/25978 K. / Aynı yönde bkz. Yargıtay 8. CD 2012/33557 E. 2013/25987 K.
[556] Yargıtay 11. CD 2010/5864 E. 2013/389 K. / Aynı yönde bkz. Yargıtay 8. CD 2016/3794 E. 2017/1405 K.

yayımlayıp, mağdurun facebook hesabına erişimini engellemesi biçiminde sübut bulan eylemlerinin TCK'nın 244/2. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme ve aynı Kanun'un 134/2. madde ve fıkrasındaki özel hayatın gizliliğini ihlal suçlarını oluşturduğuna dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir. …''[557]

şeklindeki kararda ise şifre kırılarak kişisel verilerin elde edilmesi, sisteme yetkisiz olarak erişilmesi, sistemdeki verilerin şifre değiştirilerek erişilmez kılınması, görüntülerin yayınlanması ile hem verilerin değiştirilmesi ve hem de özel hayatın gizliliğinin ihlal edilmesi durumunda; TCK md. 244 ve 134 yönünden gerçek içtima uygulamış, TCK md. 136 yönünden hiçbir değerlendirme yapmamış ve TCK md. 243'ü sanıyoruz ki yine TCK md. 244'ün bir unsuru olarak görerek bileşik suça dair normu uygulamıştır. Benzer olaylarda sistemde değiştirilen veriler ve yapılan yazışmalar özel hayatın gizliliğini ihlal etmemiş ve dolandırıcılık için yapılmış ise Yargıtay bu durumda da salt TCK md. 244 ve dolandırıcılık suçları yönünden gerçek içtima uygulamakta, TCK md. 136 ve 243'ü değerlendirme dışı bırakmaktadır.[558]

5.3.2.1.1.3. Bilişim Sistemleri Kullanılması Suretiyle Hırsızlık ve Bilişim Sistemleri Aracılığıyla Nitelikli Dolandırıcılık Suçları

Doktrinde TCK md. 243'ün bilişim sistemleri kullanılması suretiyle hırsızlık suçu yönünden bir geçit suçu olabileceği ve amaç suçtan cezalandırma yapılması gerektiği yönünde görüşler mevcuttur.[559] Farklı bir görüş ise nitelikli hırsızlık suçunda sisteme erişimin hırsızlık suçunun maddi unsuruna konu bir fiil olduğu ve bu sebeple bileşik suç hükümlerinin tatbik edilmesi gerektiği yönündedir.[560] Geçit suçu görüşü tartışılabilir ise de TCK md. 142/2'de başkasının sistemine yetkisiz olarak erişmek fiili suçun bir unsuru olarak düzenlenmediğinden ve suçta araç olarak kullanılan bilişim sistemine hukuka uygun biçimde erişilmesi de mümkün olduğundan, bileşik suç görüşüne katılmak mümkün değildir. Bu suçun işlenebilmesi için başkasına ait bir bilişim sistemine yetkili olarak erişilebileceği gibi kişi kendi sistemi üzerinden de bir kripto para cüzdanına ya da bir IBAN'a coin/para yollamaya yarayan bir zararlı kod hazırlayarak maile-siteye-linke bu zararlı kodu gömmek suretiyle hırsızlık neticesine

[557] Yargıtay 12. CD 2015/13308 E. 2017/4272 K.
[558] Yargıtay 15. CD 2017/26427 E. 2020/10070 K.; Yargıtay 15. CD 2017/31402 E. 2021/2248 K.; Yargıtay 15. CD 2017/35450 E. 2021/4698 K.
[559] Doğan SOYASLAN 2020b, age. s. 665.
[560] Ali KARAGÜLMEZ 2014, age. 218; Meral EKİCİ ŞAHİN ve Irmak KORUCULU 2019, age. s. 619, 620.

ulaşabilir. Öyleyse yetkisiz erişim fiili ile nitelikli hırsızlık suçu arasında daimi bir bağımlılığın olmadığı açıktır. Durum böyle olmakla birlikte, Yargıtay uygulaması da bileşik suçun oluştuğu yönündedir. Zira Yargıtay ilgili kısmı,

> ‘’*… Katılan ... ticari ünvanlı şirkete ait olduğu bildirilen ..." e-mail hesabına, anılan şirketle hiçbir bağlantısı, hak ve yetkisi olmadığı halde elektronik ortamda erişim sağlayan-sağlatan sanığın, katılan şirket müşterilerinden olduğu ileri sürülen, e-mail muhatabı ....hu" adresine İngilizce yazılan mesaj ile "...Ltd. e-mail adresinin vergisel manada limitini doldurduğunu ve ödenecek her meblağın şirket üzerinde fazladan vergi yükü oluşturacağını, ödemenin aşağıda belirtilen hesap no'suna yapılması gerektiği..." izahatı yapıp .. Bağlı şube nezdinde kendi adına açık olan ... no'lu hesap numarasını vererek, 24/02/2014 tarihinde ... Time ... K adlı göndericiden komisyon dahil 24.197,12 USD'nin şahsi hesabına aktarımını sağlaması-sağlatması ve 25/02/2014 tarihinde de bu paranın 7.984 USD'lik kısmını çekmesi eylemlerinin "Nitelikli dolandırıcılık", "sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçlarını oluşturduğu iddia edilen somut olayda; Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin soruşturma-kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre sanık müdafiinin yerinde görülmeyen sair temyiz itirazlarının reddine, ancak; Sanığın, katılan şirketin e-mail hesabına hukuka aykırı erişim sağlayıp şirket müşterisinin ödemesini, kendi açtırdığı banka hesabına yaptırması suretiyle haksız yarar sağlaması şeklinde iddia ve kabul edilen eyleminin Yargıtay C.G.K.'nın 17/11/2009 tarih ve 11/193-268 sayılı kararında açıklandığı üzere TCK'nın 142/2 e maddesinde tanımlanan "bilişim sistemi kullanılmak suretiyle hırsızlık" suçunu oluşturacağı nazara alınmadan suç vasfının tayininde yanılgıya düşülerek yazılı biçimde hüküm tesisi …*‘’[561]

şeklinde olan kararında, önce mail hesabına yetkisiz erişilmiş olmasını ve mail hesabından yazışma yapılarak verinin değiştirilmesi ile nihayetinde paranın yanlış hesaba gönderilerek çalınması sonucunu yalnızca nitelikli hırsızlık olarak değerlendirmiştir.[562] Her ne kadar TCK md. 244’e konu veri değiştirme/yazışma ile

---

[561] Yargıtay 15. CD 2015/8545 E. 2015/25933 K.

[562] Ayrıca bkz. ‘’*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 ... 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 nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında; 244. maddenin 4. fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır*. …‘’ Yargıtay CGK, 2009/193 E. 2009/268 K. / Aynı yönde bkz. Yargıtay CGK 2013/448 E. 2014/524

hırsızlık suçu yönünden fikri içtima uygulanması gerekiyor ise de TCK md. 243'ün neden tartışılmadığı bu karar yönünden de anlaşılamamaktadır. Sanıyoruz ki Yargıtay bu noktada da yetkisiz erişimi diğer suçların bir unsuru olarak değerlendirerek, bileşik suç hükümlerini uygulamıştır.

Yargıtay genel olarak bir bilişim sisteminin şifresi kırıldığında, elde edilen şifre ile sisteme erişildiğinde ve sistemden yazışmalar gerçekleştirilerek dolandırıcılık yapıldığında da TCK md. 136 ve TCK md. 243 yönünden bir değerlendirme yapmamaktadır. Örneğin İlgili kısmı,

> ''*… Oluşa ve dosya kapsamına göre; katılana ait e-posta adresinin şifresini kırıp bu adresteki katılanın arkadaşlarıyla katılan gibi yazışarak kendine yarar sağlamak amacı ile para talep etme şeklinde gerçekleşen eylemin, TCK.nun 244/2. maddesinde düzenlenen bilişim sistemindeki verileri değiştirme ve erişilmez kılma suçunun yanında, ayrıca TCK.nun 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılığa teşebbüs suçunu oluşturup oluşturmayacağına ilişkin delilleri takdir ve tartışmanın 5235 sayılı Adlı Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 12. maddesi uyarınca ağır ceza mahkemesinin görevinde bulunduğu gözetilerek görevsizlik kararı verilmesi gerekirken, yargılamaya devamla yazılı biçimde hüküm kurulması, …*''

şeklinde olan karar bu yöndedir.[563]

Yukarıda aktarıldığı üzere Yargıtay'ın genel eğilimi TCK md. 136 ve tez konusu olan TCK md. 243 yönünden bir şekilde bu suçların oluşmadığı yönündedir. Ancak istisnai bir kararda Yargıtay,

> ''*… Oluşa ve dosya kapsamına göre, katılanın facebook sayfasının şifresini kırarak ilgili adresteki kişilerle katılan gibi yazışarak kendine yarar sağlamak amacı ile para talep edip haksız menfaat sağlama şeklinde gerçekleşen eyleminin, bilişim sistemine*

K.; Yargıtay 17. CD 2019/2285 E. 2019/3305 K.; Yargıtay 15. CD 2014/9705 E. 2014/17102 K.; Yargıtay 15. CD 2017/5024 E. 2019/8191 K.; Yargıtay 15. CD 2020/8820 E. 2021/6281 K.; Yargıtay 15. CD 2018/8279 E. 2021/7127 K.; Yargıtay 13. CD 2013/19796 E. 2014/18903 K.; Yargıtay 11. CD 2007/8423 E. 2008/117 K.; Yargıtay 11. CD 2009/3019 E. 2009/6644 K.; Yargıtay 9. CD 2007/6709 E. 6012 K.; Yargıtay 8. CD 2014/31977 E. 2015/7086 K.; Yargıtay 8. CD 2015/12269 E. 2015/22470 K.; Yargıtay 8. CD 2016/4373 E. 2016/8431 K.; Yargıtay 8. CD 2019/20757 E. 2020/536 K.; Yargıtay 8. CD 2019/19845 E. 2020/16153 K.; Yargıtay 8. CD 2021/4526 E. 2021/15003 K.; Yargıtay 8. CD 2021/4365 E. 2021/14979 K.; Yargıtay 8. CD 2020/14787 E. 2021/15480 K.; Yargıtay 8. CD 2021/2250 E. 2021/17150 K.; Yargıtay 8. CD 2021/3475 E. 2021/17155 K.; Yargıtay 8. CD 2021/10794 E. 2021/19628 K.; Yargıtay 8. CD 2021/754 E. 2021/20284 K.; Yargıtay 8. CD 2021/6228 E. 2021/20714 K.; Yargıtay 8. CD 2019/9478 E. 2020/15892 K.; Yargıtay 6. CD 2013/35219 E. 2014/12749 K.; Yargıtay 6. CD 2021/190 E. 2021/15125 K.; Yargıtay 2. CD 2016/17834 E. 2018/887 K.; Yargıtay 2. CD 2014/18249 E. 2015/22309 K.; İstanbul Bölge Adliye Mahkemesi 9. CD 2017/718 E. 2017/924 K.

[563] Yargıtay 8. CD 2015/8 E. 2015/12695 K. / Benzer yönde bkz. Yargıtay 15. CD 2012/18643 E. 2014/11102 K.

*hukuka aykırı girmek suçu **yanında** TCK.nun 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu da oluşturup oluşturmayacağına ilişkin delilleri takdir ve tartışmanın 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 12. maddesi uyarınca ağır ceza mahkemesinin görevinde bulunduğu gözetilerek görevsizlik kararı verilmesi gerekirken, yargılamaya devamla yazılı biçimde hüküm kurulması …*''

şeklindeki değerlendirmesi ile TCK md. 136'yı yine es geçmiş olsa da[564] yetkisiz erişim suçu yönünden gerçek içtimanın gündeme gelebileceğine karar vermiştir.[565]

5.3.2.1.2. Değerlendirme

İşbu tez kapsamında detaylı olarak yetkisiz erişim suçunun objektif tipikliği ve korumayı amaçladığı değerlerin ne olduğu aktarıldı. Bu bilgiler ve yukarıda içtima yönünden değerlendirmeye alınan suçların unsurları birlikte değerlendirildiğinde ortaya çıkan ilk sonuç, bu suçlardan hiçbirine konu fiillerin TCK md. 243'ün bir unsuru olmadığı ve TCK md. 243'e konu fiilin de bu suçlardan hiçbirinin objektif tipikliğine konu bir unsur olmadığıdır.[566] İkinci sonuç ise TCK md. 243'te düzenlenen yetkisiz erişim suçunun korumayı amaçladığı değerler ile TCK md. 244/2 haricindeki suçlar yönünden bir ortaklık bulunmadığıdır. Öyleyse içtimaya konu suçlar arasında bileşik suç hükümlerinin hiçbir şekilde uygulanmaması, geçit suça dair teorinin ise TCK md. 244/2'yi oluşturacak bir kısım olaylar haricinde tatbik edilmemesi gerekir. İçtimaya konu suçlar yönünden gündeme gelebilecek diğer bir husus ise yine istisnai durumlarda fikri içtimadır.

5.3.2.1.2.1. Fikri İçtima

TCK md. 44'te düzenlenen fikri içtimanın söz konusu olabilmesi için normda açık olarak şart koşulduğu üzere ''*tek bir fiil ile birden farklı suçun*'' oluşması gerekir. Sisteme yetkisiz olarak erişildikten sonra dolandırıcılık yahut hırsızlık yapılması, özel hayatın veya haberleşmenin gizliliğini ihlal edecek şekilde veri dosyalarının açılması

[564] Uygulamada TCK md. 136'yı es geçmeyen ve dikkate almasına rağmen bu suçun oluşmayacağını belirten, buna dair gerekçesi ise kanaatimizce pek açık olmayan kararlar da mevcuttur. Bkz. İstanbul Bölge Adliye Mahkemesi 9. CD 2017/718 E. 2017/924 K.
[565] Yargıtay 8. CD 2016/1875 E. 2016/6408 K.
[566] Aynı yönde bkz. Ramazan DOĞAN 2014, age. s. 100.

yahut sistemdeki kişisel verilerin ele geçirilmesi ya da verilerin silinmesi/değiştirilmesi/erişilmez kılınması gibi durumlarda tek bir fiilin söz konusu olmadığı açıktır. Zira nasıl ki bir kişiyi hürriyetinden yoksun bırakıp odada sandalyeye bağlayan fail esirinin cüzdanını gasp edip bir de kolundaki saati zarar vermek için yere atarak kırdığında, bunlar mütemadi bir şekilde işlenen tek bir hürriyetten yoksun kılma fiili içerisinde değerlendirilmiyorlar ise TCK md. 243 bağlamında yetkisiz olarak erişilen sistemde sair suçlara yönelik gerçekleştirilen icrai fiiller de aynı şekilde tek bir fiil olarak değerlendirilemez. Öyleyse bu tür durumlarda fikri içtimanın uygulanması mümkün olmadığından, gerçek içtima gereği her suçtan ayrı ayrı ceza verilmelidir.[567]

TCK md. 244'teki neticelere sebep olma yönünden, *TCK md. 243/3'teki neticesi sebebiyle ağırlaşmış suç düzenlemesi gibi taksirle sebep olunan neticeler haricinde*, sisteme erişime dair tek bir fiil ile sistemin bozulması, verilerin değişmesi ya da aktarılması gibi neticelere ancak istisnai durumlarda sebep olunabilir. Örneğin TCK md. 244/1'de yer alan bir netice olan sistemin işleyişinin engellenmesi, brute force saldırısında kullanılan yazılımın DoS etkisi yaratması sonucu tek fiil ile mümkün olabilir ve bu sayede brute force yazılımın çalıştırılmasına dair tek fiil ile TCK md. 243 ve 244'teki neticeler doğmuş olur. Eğer failde her iki suça yönelik kast mevcut ise bu durumda fikri içtima uygulanacaktır. Özellikle bu tür istisnai durumlarda fail sisteme yetkisiz olarak erişmeye çalışırken, TCK md. 243/1'deki suçun teşebbüs aşamasında kalması fakat olası kast ya da doğrudan kastla ayrıca aynı fiil ile sistemin ya da verilerin bozulmasına sebep olması da gündeme gelebilir.

Tek bir yetkisiz erişim fiilinin birden fazla suça sebep olabilmesi; haberleşmenin gizliliğini ihlal, özel hayatın gizliliğini ihlal ve kişisel verileri hukuka aykırı olarak ele geçirme suçları yönünden salt bazı istisnai durumlarda gündeme gelebilir. Bunun için de haberleşmenin gizliliğini ihlal ve özel hayatın gizliliğini ihlal suçları yönünden, failin yetkisiz olarak eriştiği sistemde herhangi bir dosyayı icrai hareketlerle açmaması ve örneğin fotoğrafları, mailleri ''aç komutu vererek'' incelememiş olması gerekir. Zira aç komutu verildiği anda ikinci bir fiil oluşacak, bu da fikri içtimanın oluşumunu engelleyecektir. Fikri içtimanın uygulanmasına örnek olarak, failin yetkisiz şekilde eriştiği bir bilgisayarda, masaüstü arka plan resminin özel hayatın gizliliği kapsamında kalması ve hiçbir ek fiil gerçekleştirmeden failin direkt olarak özel hayatın gizliliğini de ihlal etmesi durumu verilebilir. Yine fail yetkisiz

[567] TCK md. 132-134-136 yönünden benzer görüşler için bkz. Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 249.

olarak eriştiği bir cep telefonuna erişimini sürdürürken gelen bir mesaj yahut mailin bir kısmı veya tamamı ekranda göründüğünde, tek bir fiil ile birden fazla suçun oluşumuna sebebiyet verilmiş olacaktır. Bu durumda da haberleşmenin gizliliğini ihlal ve yetkisiz erişim suçları yönünden fikri içtima uygulanarak cezası ağır olandan ceza verilecektir.[568]

TCK md. 136'da düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme suçu yönünden de yukarıdaki paragrafta haberleşmenin ve özel hayatın gizliliğine dair suçlara dair yapılan açıklamalar geçerlidir. Belirtmek gerekir ki içeriğinde belirli kişiler ile ilişkilendirilmesi mümkün olmayan verileri barındıran sair bir sisteme yetkisiz olarak erişildiğinde, şüphesiz ki TCK md. 136 yönünden bir değerlendirme zarureti gündeme gelmemektedir. Aynı şekilde herhangi bir bilgiye dahi erişilmeyen, bir ağ yapısına yetkisiz olarak erişme gibi durumlarda da böyle bir değerlendirme yapmaya gerek yoktur. Lakin bu tür durumlar haricinde bir tüzel kişiye ve hatta devlet kurumuna ait bir bilişim sistemi bile olsa, sistemlere yetkisiz olarak erişildiği andan itibaren her an bir kişisel veri ile ister istemez karşılaşmak ve bu karşılaşmalar da gayri meşru olduğu için hukuka aykırı olarak ele geçirme durumunun oluşması olasılığı çok kuvvetlidir. Zira sistem içerisinde spesifik bir dosyaya ''aç komutu'' verilmeden veya verilere dair benzer icrai hareketlerde bulunmadan dahi 6698 s. Kanun'da ''*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*'' şeklinde tanımlanan kişisel veriler ile karşılaşılması mümkündür. İşletim sisteminde kaç adet yetkili kullanıcı girişi bulunduğu, sistemde hangi uygulama yazılımlarının yüklü olduğu, klasörler üzerinde yapılan özel isimlendirmeler ya da arka plan resminin dahi kişisel veri sayılması mümkündür. Örneğin failin sisteme eriştiği anda karşısına TC kimlik numarası ile isimlendirilmiş bir klasörün ya da kişisel verilerin yer aldığı bir ekran arka plan resminin çıkması durumunda, bu kişisel verilere erişmek için ayrıca kasten bir icrai harekette bulunulmadığı için fikri içtima uygulanacaktır.

Yukarıdaki iki paragrafta TCK md. 132, 133 ve 134 yönünden verilen örnekler daha çok olası kast durumunda değerlendirilebilecek örneklerdir. Lakin eğer fail karşılıklı olarak mail alışverişi yapıldığını bildiği ve önceden malware yüklenmiş durumdaki bir sisteme bu mailleri okumak amacıyla ağ üzerinden erişir ve ekranı,

[568] Bu tür durumlarda yetkisiz erişim haricindeki suçun sübjektif tipikliği yönünden pekala bir kast karinesi gündeme gelemeyeceğinden, bu ikinci suçların daimi olarak meydana geleceği söylenemez. Ancak başkasına ait kişisel kullanıma dair bir bilgisayar ya da telefona erişerek, içeriğindeki verileri ekranında görebileceği şekilde işlemler gerçekleştiren faillerde olası kastın bulunması kuvvetle muhtemeldir.

dolayısıyla da mail içeriklerini ayrıca herhangi bir icrai hareket yapmadan olduğu gibi görür ise burada doğrudan kastla işlenen iki ayrı suç mevcut olacaktır. Yine özel hayatın gizliliğini ihlal noktasında verilebilecek en tipik örnek, IP kameraya ağ yüzerinden yetkisiz olarak erişilmesi ve evin içinin erişim gerçekleştiği an direkt olarak kasten gözlenmesidir. Yine ‘’kayıtlı üyelere dair bilgiler‘’ ile ilgili olduğunu bildiği bir veri tabanına ağ üzerinden SQL enjeksiyon saldırısı gerçekleştirdiği sırada tek bir hareketi ile hedef sunucuya SQL komutu yollayan fail, dönen cevap ile doğrudan veri tabanına yetkisiz erişim sağlamış ve veri tabanı içeriğindeki kişisel verileri de hukuka aykırı olarak ele geçirmiş, iki suçu da doğrudan kastla ve tek fiil ile işlemiş olacaktır. Tüm bu örneklerde ise fikri içtimanın uygulanması ve cezası en ağır olan suçtan cezalandırma yapılması gerekmektedir.

5.3.2.1.2.2. Geçit Suçu

Doktrinde geçit suçu teorisi gereğince, amaç suçun işlenmesi için araç suçun da işlenmesi/araç suçtan geçilmesi gerektiği durumların özellikle TCK md. 244 yönünden yaşanabileceğine ve bu durumda salt amaç suçtan cezalandırma yapılacağına dair mevcut olan görüşler yukarıda aktarıldı. Bir bilişim sistemine yetkisiz olarak erişildikten sonra sistemde yapılan işlemler sonucu başka bir suçun da kasten işlenmesi ve failin sisteme girme niyetinin de esasında bu ikinci suçu işlemek olduğu durumlar salt TCK md. 244 veya yukarıda içtima yönünden değerlendirilen suçlar bakımından değil, esasında TCK’daki pek çok suç yönünden mümkün olabilir. Zira fail delil karartma amacıyla bir sisteme yetkisiz olarak erişebilir, başkasının hesabından hasmına hakaret etmek için bu işlemi yapabilir, casusluk amacıyla faaliyetlerde bulunabilir, başkasının hapse girmesi için bilişim sistemine delil yerleştirmek yani suç uydurmak maksadıyla yahut sair pek çok sebeple de bu işlemler gerçekleştirilebilir. Geçit suçu teorisinin tüm bu sair durumlar değil de ağırlıklı olarak TCK md. 244 özelinde tartışılıyor olmasının sebebi, bu teoride daha ağır cezayı öngören amaç suçtan tek bir cezalandırma yapılmasının şartı ve gerekçesinin, her iki suçun da korumayı amaçladığı değerlerin aynı olması gereğidir.[569] Bu durum da kanaatimizce tez konusu suç yönünden salt TCK md. 244/2 yönünden mevzubahis olabilir. Bu sebeple aşağıda geçit suçuna yönelik tartışma salt bu norm yönünden yapılmıştır.

[569] Cengiz APAYDIN 2017, age. s. 90, 91; Murat Volkan DÜLGER 2021, age. s. 829; Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 649.

Geçitli suçlarda failin ulaşmak istediği esas neticenin ve esas amacın gerçekleştirilmesi için başka bir suç da ‘’nihai amaca dair geçit görevi görmesi için‘’ işlenir. Öyleyse evvela failin nihai amacının TCK md. 244/2’deki neticeleri gerçekleştirmek olmadığı, sisteme yetkisiz olarak eriştiği sırada bir anda aklında böyle bir suç işleme kastı belirmesi durumunda geçit suçuna dair teorinin uygulanması mümkün olmayacak ve gerçek içtima gereğince her iki suçtan da ceza verilecektir.[570] İkinci olarak geçit suçu teorisinde her durumda olmasa da suça konu olay özelinde amaç suçun işlenmesi için araç suçtan geçilmesinin zaruri olması şartı aranır.[571] Bu noktada tekrar hatırlatmak gerekir ki bir bilişim sisteminin çalışmasının aksatılması, bozulması, içerisindeki verilerin başka yere aktarılması, silinmesi, değiştirilmesi, erişilmez kılınması veya sisteme veri yerleştirilmesi için hedef sisteme erişilmesine objektif olarak hiçbir gerek yoktur. Zaten sistemde hakimiyet sağlamayan virüs ya da benzer nitelikteki malwarelerin gerçekleştirdiği işlemler, xss ve sair kod enjeksiyonları, DoS-DDoS atakları, taşma saldırıları ve sair pek çok hacking yönteminin neticesinde bir sisteme erişilmeden tüm bu neticelere sebep olunabilmektedir. Kanaatimizce buradaki zaruret objektif olarak algılanmalı ve sisteme erişmeden de gerçekleştirilebilecek neticeler açısından, fail bu neticeleri sisteme eriştikten sonra gerçekleştirmiş ise gerçek içtima uygulanmalıdır.

Objektif olarak bir zaruret durumunun varlığının ise her durumda TCK md. 244/2’de düzenlenen verileri değiştirme, silme, erişilmez kılma yönünden ayrıca tartışılması gerekir. Zira örneğin belirli dosya uzantısına sahip spesifik verileri bozan ya da erişilmez kılan malwareler kullanılarak örneğin bir Word dosyasının erişilmez kılınması yahut bozulması mümkün olduğundan, failin ayrıca sisteme yetkisiz olarak erişerek bu filleri gerçekleştirmesi noktasında objektif bir zaruret bulunduğu söylenemez. Aynı şekilde zararlı kodların kullanımı ile hedef sisteme yetkisiz olarak erişmeden otomatik olarak belirli bir verinin gönderimi pekala mümkün olduğundan yine herhangi bir zaruret bulunmayabilir. Bir verinin belirli bir yönde değiştirilmek istenmesi durumu ise TCK md. 244/2 yönünden TCK md. 243/1’in objektif açıdan zaruri bir geçit olabilmesi noktasında temel bir örnek teşkil edecektir. Zira sisteme erişim yetkisi olmayan bir fail tarafından ödeme kayıtlarının, üye bilgilerinin, sicil kayıtları ve sair verilerin rastgele sonuçlar doğuracak şekilde değil belirli bir sonuca yönelik değiştirilmesinin sisteme yetkisiz olarak erişmeden yapılabilmesinin pek

[570] Murat Volkan DÜLGER 2021, age. s. 829; Sulhi DÖNMEZER ve Sahir ERMAN 2019, age. s. 650.
[571] Murat Volkan DÜLGER 2021, age. s. 829.

mümkün olmadığı kanaatindeyiz. Aynı şekilde ransomware faaliyetlerinin ötesinde sistemdeki spesifik bir verinin kriptolanarak erişilmez kılınması ya da örneğin salt veri tabanındaki bir sözleşmeye dair e-imzalı pdf'in bozularak e-imzanın kaldırılması gibi durumlar yönünden de her ne kadar bu amaçlara yönelik belki çok istisnai malwarelerin üretilmesi teoride mümkün olsa da kanaatimizce bu neticelere sisteme yetkisiz olarak erişmeden ulaşmak objektif açıdan mümkün değildir. Öyleyse eğer geçit suçuna dair teori benimseniyor ise TCK md. 244/2 yönünden yetkisiz erişim suçunun yalnızca bu tür durumlarda bir araç/geçit suç sayılabileceği söylenebilir.

Kanaatimizce TCK'da açıkça düzenlenmeyen bir durumun suçların içtimaı yönünden uygulanması ve herhangi bir normatif dayanak olmaksızın ''geçit olduğuna karar verilen'' suçtan ayrıca ceza verilmeyeceğine hükmedilmesi sağlıklı bir uygulama değildir. Cezalandırmada adaletsiz bir durum olduğu düşünülüyor ise bunun doktrin ya da içtihatlar ile değil, toplumdan alınan yasama yetkisi ile yürürlüğe konulan kanunlar vasıtasıyla düzeltilmesi ve toplum/kamu adına gerçekleştirilen ceza yargılamalarında adaletin de bu şekilde sağlanması gerekir. İkinci olarak, amaç suç-araç suç şeklindeki ayrımın sübjektif olarak bazı suçlarda doktrin ve uygulamada değerlendirmeye alınırken, sair suçlar yönünden değerlendirmeye alınmadığı görülmektedir. Örneğin mala zarar verme ile konut dokunulmazlığı ihlal edilmeden çalınması mümkün olmayan evin içindeki dolapta bulunan bir obje, eve girme yetkisi bulunmayan(*ör. davet edilmeyen*) bir fail tarafından kapı kırılarak çalındığında, sair suçlar hırsızlık suçu yönünden geçit suçudur denilmemekte ve her üç suçtan da ceza verilmektedir.[572]

5.3.2.1.2.3. Sonuç

Netice olarak şahsi kanaatimiz, yetkisiz erişim suçu ve sair suçlar yönünden eğer fikri içtima uygulanamıyorsa, gerçek içtima uygulanarak her iki suçtan da ayrı ayrı ceza verilmesi gerektiği yönündedir.[573] Geçit suçu teorisinin değil, gerçek içtimanın uygulanması ceza adaleti yönünden de olumlu olacaktır. Zira farklı fiiller ile iki ayrı suç işlenmekte ve korunan değer iki ayrı suça konu iki ayrı fiilin işlenmesi sebebiyle mükerrer defalar ihlal edilmektedir. Böyle bir durumda aynı değeri bir kere

[572] Bu sonuç doğrudan TCK md. 142/4'ün lafzından doğduğu gibi Yargıtay uygulaması da bu yöndedir. Bkz. Yargıtay CGK 2014/484 E. 2016/108 K. / AYM 2008/14 E. 2010/51 K. sayılı kararında da aynı sonuca ulaşmaktadır.
[573] Benzer görüşler için bkz. Berrin AKBULUT 2017, age. s. 152, 153.

ihlal eden fail ile iki defa ihlal eden failin benzer biçimde tek suç üzerinden cezalandırılması esas adaletsizliği doğuracaktır.

5.3.2.2. Araya Girme Suçu

TCK md. 243/4'te düzenlenen araya girme suçu, iletişimin tarafı olan bilişim sistemlerine erişilmeksizin, bu sistemler arasındaki veri nakillerini/trafiğini hukuka aykırı olarak izlemektir. İçtima yönünden değerlendirilebilecek suçlara değinmeden önce belirtmek gerekir ki işbu tez kapsamında mükerrer defalar zikredildiği ve hacking yöntemleri arasında açıklandığı üzere iki sistem arasındaki trafiği bunlardan birine erişmeden izlemek için üçüncü bir sisteme yetkisiz olarak erişilebilir. Böyle bir durumda TCK md. 243/1 ve 243/4 arasında ne fiilin tekliği ne bileşik suç durumu ne de geçit suçunun şartları bulunmadığından, direkt olarak gerçek içtima gereğince her iki suçtan da ceza verilmelidir.

Araya girme suçuna konu fiil ''*nakil halindeki verileri teknik araçla izlemek*'' olduğundan, TCK'da bu fiili gerçekleştirmeden işlenemeyen herhangi bir suç bulunmadığı ve bu fiil herhangi bir suçun unsuru olmadığı için TCK md. 243/4'ün herhangi bir durumda bileşik suç içerisinde değerlendirilemeyeceğini düşünüyoruz.

Fikri içtima konusunda değerlendirmeler yapmak gerekirse, araya girme suçunun işlenmesi sırasında tek fiil ile pek çok farklı suçun oluşması mümkündür. Normun lafzında paket başlıkları yahut dar manadaki trafik bilgisi yönünden bir sınırlandırma getirilmediği için veri katmanlarının hangi derecede izlendiği bu noktada önemlidir. Eğer WAN üzerinde DPI, LAN üzerinde de paket içeriklerine direkt erişebilen ve verilerin özündeki bilgilere ulaşabilen bir teknoloji kullanılmıyorsa, böyle bir izleme faaliyeti ancak paket başlıkları ve trafiğe dair genel bilginin elde edilmesi sonucunu doğuracaktır. Bu tür genel bilgiler eğer gerçek kişiler ile ilişkilendirilebiliyor ve kişisel veri olarak nitelendirilebiliyor ise bu durumda tek fiil ile hem TCK md. 136 hem de TCK md. 243/4 oluşacak, fikri içtimanın uygulanması sonucu cezası en ağır olan suçtan ceza verilecektir.

WAN üzerinde DPI, LAN üzerinde de paket içeriklerine direkt erişebilen ve verilerin özündeki bilgilere ulaşabilen bir teknoloji kullanıldığı zaman direkt olarak erişilen bilgiler noktasında ikili bir ayrım yapmak gerekir. Eğer trafik kriptolanmışsa, bu durumda kriptografik kodlamalara ulaşılacağı ve anahtar girilmeden gerçek bilgi öğrenilemeyeceği için bu durumun kişisel veriler nazarında tartışılması gerekir. Her ne kadar algoritmalar kırılabiliyor, anahtarlar çalınabiliyor ve hatta kriptografik

kodlamalar yorumlanarak içerdiği bilgi tahmin edilebiliyor olsa da kanaatimizce bunlar birer kişisel veri sayılmamalıdır. Öyleyse verilerin içeriğindeki bilgilere erişilse bile karşılaşılan bilgi kriptolanmış ise yalnızca TCK md. 243/4 oluşacağı için içtima yönünden bir değerlendirmeye gerek olmayacaktır. Trafiğin kriptosuz akması durumunda veya veri trafiğini izleyip analiz etmek için kullanılan yazılım otomatik olarak kriptoyu da kırabiliyor ise bu şekilde tek fiil ile iki ayrı suç oluşacaktır. Ulaşılan bilgilerin niteliğine göre TCK md. 243/4'e ek olarak işlenen suçun, iletişim iki gerçek kişi arasında yapılıyor ve haberleşmenin gizliliği kapsamında kalıyor ise md. 132, özel hayatın gizliliği kapsamında kalıyor ise md. 134, kişisel verilerin gizliliği kapsamında kalıyor ise md. 136'da düzenlenen suç olması muhtemeldir. Bu durumda iki suç da tek fiil ile gerçekleştirildiği için TCK md. 44 gereğince fikri içtima uygulanacak ve cezası en ağır olandan ceza verilecektir.[574] Eğer veri trafiği izlenirken paketler yakalandıktan sonra içeriklerine otomatik olarak erişilir fakat kriptonun kırılması için ayrık olarak başka fiiller gerçekleştirilir ise bu durumda ortada tek fiil oluşmayacağı için gerçek içtima gereği her iki suçtan da ayrı ayrı ceza verilmesi gerekir.

5.4. CEZA VE GÜVENLİK TEDBİRLERİ

5.4.1. Cezalar

5.4.1.1. TCK md. 243'te Düzenlenen Suçların Cezaları

Yetkisiz erişim suçunun temel halinde TCK md. 243/1 gereğince bir yıla kadar hapis veya adli para cezasına hükmedilir. Suçun konusu bedeli karşılığı yararlanılabilen sistemler olduğunda ise verilecek ceza ikinci fıkraya göre yarı oranına kadar indirilecektir. Üçüncü fıkrada düzenlenen yetkisiz erişim suçunun neticesi sebebiyle ağırlaşmış halinde ise altı aydan iki yıla kadar hapis cezasına hükmolunur. Araya girme suçunun işlenmesi halinde de TCK md. 243/4'e göre bir yıldan üç yıla kadar hapis cezası verilecektir. Terörle Mücadele Kanunu md. 5'e göre yetkisiz erişim ve araya girme suçları terör amacı ile işlenmişse, verilecek hapis veya adli para cezaları yarı oranında artırılacaktır.[575]

---

[574] Aynı yönde bkz. Nagihan GÜN 2020, age. s. 208; Köksal BAYRAKTAR, Zeynel T. KANGAL vd. (Ali Kemal YILDIZ) 2021, age. s. 249; Berrin AKBULUT 2017, age. s. 170 / Doktrinde TCK md. 243/4'te düzenlenen araya girme suçunun işlenmesi sırasında kişisel veriler de hukuka aykırı olarak ele geçirilmiş ise daima gerçek içtimanın uygulanacağını belirten görüşler de mevcut olup, TCK md. 44'ün açık lafzı gereğince bu görüşlere katılmıyoruz. Bu görüşlere dair bkz. Mahmut KOCA ve İlhan ÜZÜLMEZ 2020, age. s. 911; Murat Volkan DÜLGER 2022, age. s. 329.

[575] İlgili maddeye göre bu suretle tayin olunacak cezalarda gerek o fiil için gerek her nevi ceza için muayyen olan cezanın yukarı sınırı aşılabilecektir. Suçun, örgütün faaliyeti çerçevesinde işlenmiş

Yetkisiz erişim suçunda hapis ve adli para cezası seçimlik olarak öngörüldüğünden her ikisinin de birlikte verilmesi mümkün değildir.[576] Mahkumiyet durumunda hapis cezasına hükmedilirken[577] de adli para cezasına hükmedilirken de süre yönünden alt sınırdan ayrılmak için somut delillere dayalı yeterli bir gerekçelendirme yapılmalıdır.[578] Adli para cezasında miktar yönünden alt sınırdan ayrılmak için de ödeme imkanına dair gerekçelendirme yapılması gerekir.[579] Ayrıca TCK md. 61/9 gereğince adli para cezasının seçimlik olduğu suçlarda, adli para cezasına ilişkin gün biriminin alt sınırı, o suç tanımındaki hapis cezasının alt sınırından az, üst sınırı da hapis cezasının üst sınırından fazla olamaz.

5.4.1.2. Cezalara Dair Değerlendirme

TCK md. 243'teki suçlara dair cezalar yönünden doktrinde üzerinde durulan ilk husus, siber güvenlik önlemlerinin cezalandırmaya ne şekilde etki etmesi gerektiğidir. Bir görüşe göre şifre dahil hiçbir siber güvenlik önlemi alınmayan bir sisteme erişilmesi durumunda hafifletici sebebe dair bir düzenleme yapılmasının olumlu olacağı zikredilirken,[580] sair bir görüş ise böyle bir durumda hafifletici sebebin gerekmediği lakin siber güvenlik önlemleri yoğun olan bir sisteme yetkisiz olarak erişildiğinde hassas verilere erişim noktasında ağırlaştırıcı sebep düzenlemesine gidilmesi gerektiği yönündedir.[581]

Kanaatimizce verilere dair bilgiler ve bu bilgilerin hassaslığı yahut kritikliği TCK md. 243/1'in koruma alanında olmadığından, böyle bir durumun TCK md. 243 değil lakin TCK md. 136 yönünden bir ağırlaştırıcı sebep olması gerekirdi. Hiçbir siber güvenlik önlemi alınmayan sistemlere yetkisiz olarak erişilmesini hafifletici sebep saymak ise bu durum korumayı amaçlanan değerlere tecavüz nazarında hiçbir hafiflik barındırmadığından, salt şanslı suçluların ödüllendirilmesine sebep olacaktır. Nasıl ki bir araba hırsızına arabaya bindiğinde anahtarı torpidoda bulduğu zaman hiç zorlanmadan anahtarı kullanıp arabayı çaldığında daha az ceza verilmiyor ise bilişim sistemine yetkisiz olarak erişmek niyetiyle eylemlere girişen failin hiçbir siber güvenlik

olması dolayısıyla ilgili maddesinde cezasının artırılması öngörülmüşse; sadece bu madde hükmüne göre cezada artırım yapılır. Ancak yapılacak artırım, cezanın üçte ikisinden az olamaz.
[576] Murat Volkan DÜLGER 2022, age. s. 315; Ali KARAGÜLMEZ 2014, age. s. 226.
[577] Yargıtay CGK 1976/7-390 E. 1976/386 K.
[578] Yargıtay CGK 2010/1-30 E. 2010/99 K.
[579] Yargıtay CGK 2013/374 E. 2014/444 K.
[580] Ali KARAGÜLMEZ 2014, age. s. 77.
[581] Murat Volkan DÜLGER 2022, age. s. 267.

önlemiyle karşılaşmaması durumunda da hafifletici bir sebep adil bir düzenleme olmayacaktır.

Doktrinde cezalandırma noktasında üzerinde durulan ikinci husus, suçun konusuna dair ağırlaştırıcı sebep düzenlemesinin olmamasıdır. Doktrinde askeri sistemlere veya kamu kurumu sistemlerine yetkisiz olarak erişilmesi durumunun bir ağırlaştırıcı sebep olarak düzenlenmesi gerektiği zikredilmektedir.[582] Bu görüşe kısmen katılıyoruz. TSK ve İç İşleri Bakanlığına bağlı jandarma ve kolluk birimlerinin bünyesindekiler ile MİT bünyesindeki bilişim sistemlerinin külli olarak bir ağırlaştırıcı sebep düzenlemesine dahil edilmesi gerekmektedir. Zira suçun korumayı amaçladığı değer yetkisiz olarak erişilemeyen sistemlere dair, sistem üzerindeki yetkiden kaynaklı haklar ve bilişim sisteminin yetkisiz erişimlere karşı dokunulmazlığıdır. Bu tür sistemlerin dokunulmazlığı ise açıktır ki sair sistemlerinkinden çok daha yüksektir. Ancak her kamu kurumu bünyesindeki sistemler yönünden böyle bir ağırlaştırıcı sebebe gerek görmüyoruz. Bu noktada esasında yukarıda zikredilen kurumların sistemlerinin de içerisinde değerlendirilebileceği çatı bir kavram olan kritik altyapılar[583] ile özellikle SCADA sistemi parçalarına dair bir ağırlaştırıcı sebep düzenlemesi yapılması gerektiğini söylemek daha doğru olacaktır. Zira bu tür sistemlerin yanlış işlemesi ekonominin, kamu düzeninin, milli güvenliğin, toplum sağlığının, enerji kullanımının veya doğanın üzerinde çok ciddi menfi etkiler doğurabilir.[584] Öyleyse bu tür sistemlerin dokunulmazlığının hukukça sair sitemlerden daha yüksek seviyede korunuyor olması gerekir. Yetkisiz erişim suçunun hafifletici sebebi olan ikinci fıkradaki düzenlemeye dair detaylı açıklamalar ilgili suça dair alt başlık altında yapıldığından, burada tekrarlanmamıştır.

Araya girme suçu yönünden ise kanunda herhangi bir ağırlaştırıcı ya da hafifletici sebep düzenlemesi bulunmamaktadır. Kanaatimizce bu suçun konusu olan nakil halindeki veriler eğer milli güvenlik, devlet sırları yahut sair kritik iletişimlere yönelik ise iletişim kriptolu olacağı için bunların içeriği çözülemese bile salt bu trafiklerin izlenmesinin haksızlık boyutu çok yüksek olacaktır. Araya girme suçunun objektif tipikliği için kriptonun çözülmesi ve hatta kriptografik kodlara ulaşılması dahi gerekmediğinden, suç trafiğin izlenmesi ile oluşacağı için casusluk yahut terör amacı

[582] Berrin AKBULUT 2017, age. s. 143.
[583] Muhammet KARACA 2019, age. s. 36, 37 vd.
[584] Semih Töner ŞEN 2021, age. s. 29, 30 vd.

gütmese bile TSK, MİT, EGM ve benzeri noktalardaki iletişimlere dair trafiğin izlenmesinin ağırlaştırıcı sebep olarak öngörülmesi gerekirdi.

Cezalar noktasında son olarak TCK md. 243/3'te düzenlenen, yetkisiz erişim suçunun neticesi sebebiyle ağırlaşmış hali için öngörülen cezaya da değinmek gerekir. Neticesi sebebiyle ağırlaşmış suç düzenlemelerinin temel mantığı, bu suçların kasten gerçekleştirilmek istenen suçtan daha ağır lakin taksirle sebep olunan neticenin tipikliğine dahil olduğu esas suçtan daha hafif bir haksızlık yaratmasıdır. Öyleyse bilişim sistemine kasten yetkisiz olarak erişildiğinde istemeden veriler yok edilmiş/bozulmuş ve TCK md. 243/3'te düzenlenen neticesi sebebiyle ağırlaşmış suça sebep olunmuş ise mantıken bu suçun cezasının TCK md. 244/2'de düzenlenen kasten bir verinin yok edilmiş/bozulmuş olmasına dair suçtan daha hafif olması gerekir. Ancak TCK md. 243/3 ile TCK md. 244/2'de düzenlenen suçlara öngörülen cezalarda alt sınır aynıdır. Alt sınırdan ayrılmak için somut delillere dayanan gerekçe lazım olduğundan, her iki suçun da sıradan biçimde işlenmesi durumunda, yetkisiz erişimden daha ağır olduğu kanun koyucu tarafından öngörülmüş ''verinin yok edilmesi ya da değiştirilmesi'' neticelerine taksirle de sebep olunsa kasten de sebep olunsa faillere aynı ceza verilecektir. Sanıyoruz ki bu durum cezalandırmaya dair adil bir vaziyet değildir. Hümanist bir ceza hukuku felsefesi benimsenir ise bu noktada TCK md. 244/2'deki cezanın alt sınırının yükseltilmesi değil, TCK md. 243/3'teki cezanın alt sınırının düşürülmesi gerekecektir.

5.4.2. Güvenlik Tedbirleri

CMK md. 223'e göre evvela mahkumiyete hükmedilmiş ise cezaya alternatif olarak veya cezaya ek olarak güvenlik tedbirine hükmolunur. İkinci olarak, fail kınanamadığı için ceza verilmesine yer olmadığına dair bir karar veriliyor ise bu durumda da bu karara ek olarak güvenlik tedbirine hükmedilebilir.[585] Yetkisiz erişim ve araya girme suçları yönünden mahkumiyet durumunda uygulanabilecek güvenlik tedbirlerini iki yönlü açıklamak doğru olacaktır. TCK md. 246'da bu suçları da içine alacak şekilde ''*Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur*'' denilmiştir. Öyleyse bu suçlar ile bir tüzel kişi yararına haksız menfaat sağlanıyor ise TCK md. 60 gereğince iznin iptali ve/veya müsadere kararı tüzel kişilere

[585] Murat BALCI, M.Emin ALŞAHİN ve Kerim ÇAKIR 2021, age. s. 619.

yönelik de verilebilecektir. İznin iptali yönünde bir güvenlik tedbirine hükmolunabilmesi için bu iznin verdiği yetkinin kötüye kullanılması gerekmektedir. Araya girme suçu yönünden bu tür bir duruma tipik örnek, yetkilendirilmiş olma şartı ile faaliyet gösteren erişim sağlayıcı anonim şirketin suça konu faaliyetleridir. Müsadere noktasında ise evvela belirtmek gerekir ki salt bu suçların neticesinde haksız bir maddi kazanç sağlanması mümkün olmadığından, kazanç müsaderesi yalnızca bu tür suçların parasal değerler karşılığı işlenmesi durumunda ''suç işleme ücretine'' yönelik olabilir. Öyleyse bu noktada önemsenmesi gereken temel husus, suç eşyalarının müsaderesine dair düzenlemelerdir.

Gerçek kişiler yönünden güvenlik tedbirleri ise evvela TCK md. 53'teki tedbirler ve müsaderedir. Kanaatimizce gerçek kişiler yönünden de bu suçlar nazarında esas önemsenmesi gereken husus, suç eşyalarının müsaderesidir. TCK md. 54'te düzenlenen eşya müsaderesi, iyi niyetli üçüncü kişilere ait değil ise suç aleti olan ve/veya suça özgülenmiş bilişim sistemlerinin CMK md. 123'e göre muhafaza altına alınmasına ya da el konulmasına ve müsadere kararının tatbiki ile bilahare bunların müsaderesine izin vermektedir. Bir şeyin sadece bazı kısımlarının müsaderesi gerektiğinde, tümüne zarar verilmeksizin bu kısmı ayırmak olanaklı ise sadece bu kısmın müsaderesine karar verilecek, birden fazla kişinin paydaş olduğu eşya hakkında ise sadece suça iştirak eden kişinin payının müsaderesine hükmolunacaktır. Ancak üçüncü fıkrada düzenlendiği üzere, suçta kullanılan eşyanın müsadere edilmesinin işlenen suça nazaran daha ağır sonuçlar doğuracağı ve bu nedenle hakkaniyete aykırı olacağı anlaşıldığında, müsaderesine hükmedilmeyebilecektir.

Bu suçlarda suçun konusu olan mağdura ait bilişim sisteminin haricinde failin kullanımındaki bilişim sistemleri ve araya girme suçu yönünden kullanılabilecek sair teknik cihazlar suç aleti konumundadır. Köle bilgisayar kullanımında iyi niyetli üçüncü kişilere ait bu sistemler her ne kadar suç aleti olsa da TCK md. 54 gereğince müsaderenin konusunu oluşturmayacaktır.[586] Failin kullandığı sistemler ve/veya teknik cihazlar ise müsaderenin konusunu oluşturmaktadır. Kanaatimizce bu noktada her suça konu olay kendi özelinde değerlendirilmelidir. Bir bilgisayar, tablet yahut cep telefonu gibi salt bu suçları işlemesi için tasarlanmayan sistemlerin suç aleti olması durumunda bunların her daim müsaderesine karar verilmemelidir. Zira bu durum suçtan daha ağır bir haksızlık yaratacak olup, TCK md. 54/3 gereğince müsadere

[586] Müsaderede kişinin iyi niyetli üçüncü kişi olup olmadığının değerlendirilmemesinin hak ihlali yaratacağı yönünde bkz. AYM, Mehmet Salih Baltacı Başvurusu, Başvuru no: 201714768.

yapılmamalıdır. Lakin eğer suçun işlenmesini kolaylaştıran bir yazılım kullanılmış ise TCK md. 54/5 gereğince kısmi müsadere yapılarak salt bu yazılımların el koyma sonrası silinmesi ve bilahare sistemin faile iadesine karar verilmesi doğru olacaktır.[587] Her ne kadar bu tür yazılımların bulundurulması TCK md. 245/A'ya göre suç ise de TCK md. 54/4'e göre direkt müsadere yapılması için ''eşya niteliği'' gerektiğinden, yazılımlar dördüncü fıkraya değil beşinci fıkraya göre müsadere edilmelidir. Fail salt bu suçların işlenmesi için tasarlanan bir bilişim sistemi yahut teknik bir cihazı suç aleti olarak kullanmışsa bu durumda eğer bu alet TCK md. 254/A'ya göre bizatihi suç teşkil ediyor ise dördüncü fıkraya, böyle bir vaziyet yok ise salt suç aleti olması gereğince birinci fıkraya göre müsadere edilecektir. Kanaatimizce eğer bu suçlara dair birden fazla tekerrür hali mevcut ise ve tekerrür eden suçlarda kullanılan suç aleti sistemler ele geçirilememiş lakin en son suçta bu başarılmış ise suç aleti bir bilgisayar dahi olsa bunun içerisindeki suç ile bağlantısız veriler faile iade edildikten sonra bilgisayarın tamamen müsaderesi hakkaniyetli olacaktır.

Müsadere kararı hüküm yani son kararda yer almaktadır. Eğer hükmün açıklanmasının geri bırakılmasına karar verilmiş ise her iki karar da hüküm fıkrasında yer alacaktır.[588] Öyleyse hükmün açıklanmasının geri bırakılması süresince müsadere işlemleri gerçekleştirilemeyecek, şartları oluşur ve hüküm açıklanmaz ise müsadere kararının da tatbiki imkansızlaşacaktır.[589] Bu durumda şüphesiz ki el konulmuş sistem ve teknik cihazların faile iadesi de gerekir.

[587] Aynı yönde bkz. Mustafa SEMİZ (2021), *Bilişim Suçları ve Soruşturma Yöntemleri*, Adalet, Ankara, s. 301.
[588] Yargıtay 7. CD 2009/9362 E. 2012/3220 K.
[589] Yargıtay 8. CD 2016/5776 E. 2016/7400 K.

SONUÇ

Yetkisiz erişim suçu, TCK md. 243'ün ilk üç fıkrasında düzenlenmiştir. Araya girme suçu ise 243. maddenin son fıkrasında düzenlenmiştir. Aynı maddede düzenlenen iki suçun da mülga ceza kanununda doğrudan bir karşılığı bulunmamaktadır. Bu suçlara dair düzenlemeler esas olarak Avrupa Siber Suçlar Sözleşmesi'nden esinlenerek yapılmış olup, yetkisiz erişim suçu ilgili sözleşmede ikinci ve araya girme suçu ise üçüncü maddelerde düzenlenmiştir. Bu sebeple TCK md. 243'ün yapısı, Avrupa Siber Suçlar Sözleşmesi ile tam bir paralellik göstermektedir.

Bilişim sistemleri, otomatik biçimde veri girdi-çıktısı yaparak veriler üzerinde çeşitli işlemler gerçekleştirilebilmesini sağlar. Temel özelliği veriler üzerinde otomatik olarak işlemler gerçekleştirmek olan bilişim sistemlerini veri boyutundan ayrık olarak düşünmek mümkün değildir. Öyleyse bilişim sistemi, donanım ve veri boyutuyla bir bütün olarak anlaşılmalıdır. Türk hukuku ve tez konusu suçlar yönünden de bilişim sistemi kavramının bu şekilde anlaşılması, aksi yönde bir normatif düzenleme olmadığı için asgari olarak verileri otomatik olarak işleyebilen ve depolayabilen teknolojik aletlerin bilişim sistemi olarak kabul edilmesi gerekmektedir.

Tez konusu suçlar genel olarak hacking faaliyetleri sonucunda işlenmektedir. Brute force saldırıları, enjeksiyon saldırıları ve botnet ağı oluşturmak, yetkisiz erişim suçuna yönelik tipik hacking faaliyetleridir. Yetkisiz erişim suçunun işlenebilmesi için phishing ile spoofing faaliyetleri de gerçekleştirilebilmekte, yetkisiz erişimin sonucunda ise DoS-DDoS atakları köle bilgisayarlardan yapılabilmekte olup, bu hacking faaliyetleri de yetkisiz erişim suçu ile yakından ilişkilidir. Araya girme suçuna yönelik tipik hacking faaliyetleri ise Man In The Middle ve sniffing yöntemleri olup, MAC-ARP Spoofing ve MAC Flooding yöntemleri ile de benzer sonuçlara ulaşılabilmektedir.

Yetkisiz erişim suçu ile korunması amaçlanan tek değer, bilişim sisteminin yetkisiz erişimlere karşı dokunulmazlığıdır. Bu suç ile kişisel veriler, özel hayatın gizliliği, mülkiyet hakkı ve sair hususun korunması amaçlanmamıştır. Kanun maddesinde ayrık bir düzenleme bulunmadığından, herkesin bu suçun faili ve mağduru olması mümkündür. Suçta mağdur sıfatı, bilişim sistemi üzerinde donanım ve siber uzayın ayrılmaz bütünlüğü noktasında bir yetkiye sahip olan kişilerde bulunabilir. Yetkisiz erişim suçunun konusu, asgari olarak verileri otomatik olarak işleyebilen ve depolayabilen teknolojik aygıtlara karşılık gelen bir kavram olarak bilişim sistemleridir. Suçun konusunu oluşturması için bilişim sistemlerinde herhangi bir siber güvenlik önlemi alınmış olması şartı bulunmamaktadır. Hukuken yetkisiz olarak erişilmeye müsait her sistemin bu suçun konusu olması mümkündür. Suçun konusu eğer bedeli karşılığı yararlanılabilen sistemler ise maddenin ikinci fıkrasına göre ceza yarı oranına kadar indirilecektir. Bu hafifletici sebep düzenlemesine dahil edilebilecek bilişim sistemlerinin, maddi bir bedel karşılığında ve üyelik/yönetici onayı sonrası erişilebilen, sistem yöneticilerinin siber güvenlik kaygıları haricinde müşterilerin kişisel özelliklerini dikkate almaksızın bedelini ödeyen herkesin talebini onaylayacağı, bedel karşılığı yararlandırılan bu hizmetin de müşteriler yönünden bir tüketici ilişkisi yarattığı hizmetlere özgülenmiş sistemlerdir. Kanun koyucunun bu şekilde bir hafifletici sebep düzenlemesi getirmesinin sebebi; bedeli karşılığı sistemler üzerindeki dokunulmazlığın kaldırıldığı durumlarda, korunması amaçlanan değer olan dokunulmazlığın ihlalinin suçun temel şeklinin işlenmesine göre daha az bir haksızlık doğuracak olmasıdır. Yetkisiz erişim suçunun hafifletici sebebe dair ikinci fıkrasının TCK md. 163'te düzenlenen karşılıksız yararlanma suçu ile lafzi bir bağlantısı mevcuttur. TCK md. 163/2 ile TCK md. 243/2 arasındaki bağlantıda, TCK md. 243/2 bilişim sistemleri yönünden özel norm durumundadır. Öyleyse karşılıksız yararlanılan sistem bilişim sistemi ise karşılıksız yararlanma suçu değil, yetkisiz erişim suçu oluşacaktır. Lakin spesifik olarak otomatları düzenleyen TCK md. 163/1, TCK md. 243/2 karşısında özel norm durumdadır. Bu sebeple otomatlar noktasında salt karşılıksız yararlanma suçu oluşacaktır.

TCK md. 243/1'de düzenlenen yetkisiz erişim suçunun temel hali, bilişim sisteminin bütününe veya bir kısmına yetkisiz olarak erişmek/girmek ve bilişim sisteminde yetkisiz olarak kalmaya devam etmek şeklinde iki seçimlik hareket ile işlenebilen bir suçtur. Neticesi harekete bitişik olan bu suç yönünden, objektif tipikliğin oluşumu için sistemdeki bilgileri öğrenme yahut sistemlere zarar verilmesi

şartı aranmamaktadır. Hareket/fiil ile netice arasına belirli bir zamanın girmesi, her iki seçimlik hareket yönünden de aranmamaktadır. Bu sebeple yetkisiz erişimin yahut kalmaya devam etme durumunun asgari bir süre devam etmesi suçun objektif tipikliğine konu bir mesele değildir. Öyleyse bu suç ani suç olarak işlenebilen lakin suç oluştuktan sonra da işlenmeye devam eden/temadi eden, muhtemel bir mütemadi suç özelliği göstermektedir. Her iki seçimlik hareket yönünden de suçun hem icrai hem de ihmali hareket ile işlenmesi mümkündür.

Donanım ve veri boyutuyla ayrılmaz bir bütünlük oluşturan bilişim sistemlerine yetkisiz olarak erişmek, siber uzaya yönelik bir erişim sonucu tecelli edebilir ve bu sebeple monitörün göz ile izlenmesi yahut bilgisayar kasasının açılması gibi faaliyetler suçun objektif tipikliğine konu fiiller değildir. Yetkisiz erişimin ne şekilde gerçekleşmiş sayılacağı noktasında çerçeve bir değerlendirme ölçütü olarak, ‘’*sistemdeki verilere ulaşma ve/veya sistem içeriğine kontrol altında bir müdahale imkanı doğduğu an*‘’ sisteme erişilmiş olunacağı kabul edilmelidir. Bu yetkinlikleri sağlayan husus bir malware çalıştırılması, kod, komut ya da veri paketi gönderimi yahut brute force sonucu bilfiil ağ üzerinden sisteme erişim veya direkt olarak fiziki bağlantılar yapılması olabilir. Sanallaştırma teknolojileri sayesinde tek bir donanım yapısında soyut olarak birbirinden ayrılmış parçalar yani sanal makineler de ayrık birer bilişim sistemi olarak kabul edilmelidir. Bu sebeple tek bir fiziki donanım içerisinde bulunsalar bile bu sistemlere ayrı ayrı erişim, farklı yetkisiz erişim suçları doğuracaktır. İçeriği sanallaştırılmamış sistemlere veya sanal birimlerin içeriğindeki farklı kısımlara erişilmesi ise tek bir sisteme erişim suçunun icrasına konu faaliyetler kapsamında değerlendirilmelidir.

Yetkisiz erişim suçunun sübjektif tipikliğinin oluşumu için kast ve hukuka aykırılık bilinci gerekmektedir. Suçun olası kastla işlenmesi teoride mümkün ise de pratikte bu durumun gerçekleşmesi pek olası değildir. Zararlı sonuçların minimize edilmesi için çeşitli testlerden geçirilmiş ve veri havuzu denetim altında bulunan yapay zeka teknolojilerinin yaratacağı sonuçlar öngörülebilir ve istenebilir durumdadır. Öyleyse deneysel ve öngörülemez yapay zeka teknolojileri haricinde, yapay zeka kullanımının yetkisiz erişim suçunun sübjektif tipiklik unsurunun oluşumuna yönelik tam bir engel teşkil ettiği söylenemez.

Yetkisiz erişim suçu ile TCK’nın lafzında yer alan bütün hukuka uygunluk sebepleri bağdaşmaktadır. Hakkın kullanılması bakımından bu yönde sözleşmeden kaynaklı haklar, velayet hakkı, işverenin sahip olduğu haklar ile telekomünikasyon

omurgasını kullanma ve omurgaya erişim durumları öne çıkmaktadır. Kanun hükmünü icra bakımından CMK md. 134'te düzenlenen arama faaliyetleri, BTK, MASAK ve SPK'nın denetim faaliyetleri ile yer sağlayıcıların 5651 s. Kanun'dan kaynaklı görevlerine dair faaliyetleri öne çıkmaktadır. Rızanın çeşitli şekillerde bu suç yönünden hukuka uygunluk sebebi teşkil etmesi mümkündür. Meşru savunmanın da teorik olarak bu suç yönünden tatbik edilmesine dair bir engel bulunmamaktadır. Suçun kınanabilirlik unsuru yönünden önemsenmesi gereken ilk husus, bir daha delil elde edemeyeceği ihtimali gereğince hareket eden faillere dair zorunluluk halinin varlığıdır. İkinci olarak, haksızlık bilincinin yokluğu suçun sübjektif tipikliğinin oluşumunu engelleyeceğinden, TCK md. 30/4'teki haksızlık bilincine dair hataya dair düzenlemenin bu suç yönünden uygulama alanı bulabilmesi mümkün değildir.

TCK md. 243/3'te yetkisiz erişim suçunun, verilerin yok olması ya da değişmesi neticelerine yönelik, kast+taksir kombinasyonunu içeren gerçek bir neticesi sebebiyle ağırlaşmış suç oluşturulmuştur. Fail yetkisiz olarak eriştiği sistemde kasten verilerin yok olması ya da değişmesine sebep olursa bu noktada TCK md. 243/3 değil, bu neticeyi tipikliğinde barındıran temel norm olan TCK md. 244/2 oluşacaktır.

TCK md. 243/4'te düzenlenen araya girme suçu ile korunması amaçlanan değer, veri trafiğinin gizliliğine dair haktır. Bu suç ile kişisel veriler ve verilerin içerdiği sair bilgilere dair haklar korunmamaktadır. Araya girme suçunun faili ve mağdurunun herkes olabilmesi mümkündür. Suçta mağdur sıfatı, veri trafiğinin taraflarında bulunacaktır. Araya girme suçunun konusu nakil halinde olan verilerdir. Bu verilerin herhangi bir elektronik haberleşme yapısında nakledilmesi mümkündür. Suça konu fiil, bu verilerin, iletişimin tarafı sistemlere erişmeksizin ve teknik araçlar kullanılarak izlenmesidir. Araya girme suçunda kullanılabilecek teknik araçların, kablolar ya da elektromanyetik dalgalar üzerinden iletilen veri paketlerini yakalayabilecek ve bu sayede veri trafiğini izlemeyi gerçekleştirecek bir cihaz olması şart olup, suça konu hareket bir ağ yapısında nakledilen veri trafiğini izlemektir. Neticesi harekete bitişik olan bu suç, izlemenin gerçekleşmesi ile oluşacak lakin izleme devam ettiği sürece suçun işlenmesi de devam edecektir. Öyleyse bu suç muhtemel mütemadi suç durumundadır. Suçun sübjektif tipikliğinin oluşumu için failde kast ve hukuka aykırılık bilincinin bulunması gerekir. Suçun olası kastla da işlenmesi mümkündür.

Araya girme suçu yönünden, meşru savunma dışında TCK'da yazılı olan bütün hukuka uygunluk sebeplerinin tatbiki mümkündür. Hakkın kullanılması noktasında

sözleşmeden doğan haklar ile işverenlerin bu konudaki hakları öne çıkmaktadır. Elektronik haberleşmede veri iletişimi birden çok taraf arasında bulunduğundan, işverenin ancak tüm tarafları işçi olan bir trafiğe dair hakkını kullanması söz konusu olabilir. Kanun hükmünü icra noktasında erişim sağlayıcılar ve toplu kullanım sağlayıcıların veri trafiğini izlemeleri ve bu şekilde normatif yükümlülüklerde bahsi geçen dar manadaki trafik bilgisini kaydetmeleri, iletişimin tespiti ve iletişimin dinlenmesine dair verilen kararların tatbiki ile MİT Kanunu'ndaki veri trafiğini izlemeye dair düzenlemeler öne çıkmaktadır. Rızanın da çeşitli şekillerde bu suç yönünden hukuka uygunluk sebebi teşkil etmesi mümkündür. Lakin iletişimin tek tarafının verdiği rıza yalnızca kendi trafiğine yönelik bilgiler yönünden bir hukuka uygunluk sebebi teşkil edebilecek olup, hedef sisteme yönelik trafik bilgisi yahut trafikteki verilerin içerdiği bilgiler yönünden tüm tarafların rızası gerekir. Suçun kınanabilirlik unsuru yönünden ise önem arz eden yahut tartışılabilecek bir husus bulunmamaktadır.

TCK md. 243'te düzenlenen tez konusu iki suç açısından da teşebbüs hükümlerinin uygulanması mümkündür. Bu suçlara iştirak yönünden ortaya konulması gereken temel husus, yetkisiz erişim suçunun neticesi sebebiyle ağırlaşmış haline iştirak için ağırlaşan neticenin faillerin suçun işlenmesine dair ortak iradelerinin sınırlarının içerisinde kalması gerektiğidir. İkinci olarak, iştirakçiler bilfiil suça yönelik karşılıklı bir anlaşma yapmasalar dahi işlenecek veya işlenmekte olan somut bir suça bilerek katkı sağlamak iştirak iradesini teşkil edecektir. Öyleyse BT çalışanlarının işlenecek veya işlenmekte olan somut bir suça yönelik siber güvenlik önlemlerini kasten askıya alması gibi durumlarda bu çalışanlar suçta iştirakçi olarak kabul edileceklerdir.

Yetkisiz erişim suçunun temel şekli, hafifletici sebebin gerçekleştiği hal ve neticesi sebebiyle ağırlaşmış şekli noktasında zincirleme suç hükümlerinin tatbiki mümkündür. Araya girme suçu yönünden de zincirleme suç hükümlerinin uygulanması olanaklıdır. Araya girme suçu yönünden zincirleme suç noktasında değerlendirilmesi gereken en önemli mesele, doğası gereği birden fazla mağdurun olduğu bu suçta, aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesine yönelik TCK md. 43/2'nin her daim uygulanmasının mümkün olmadığıdır. Bu normun tatbiki için izlenen trafiğin yani suçun konusunun farklı olması gerekir. Şüphesiz ki aynı durum yetkisiz erişim suçu yönünden de geçerlidir.

Yetkisiz erişim suçu ve araya girme suçunun işlendiği sırada farklı suçların oluşması muhtemel olduğundan, suçların içtiması yönünden titiz bir inceleme yapılması gerekmektedir. Bu suçların kendi aralarında ve TCK md. 245/A'da düzenlenen ''yasak cihaz veya programlar'' başlıklı suç ile aralarında bileşik suç, fikri içtima yahut geçit suçuna dair bir uygulamanın gündeme gelmesi mümkün değildir. Bu sebeple fiil ve neticeleri tamamen farklı olan bu suçlar arasında daima gerçek içtima uygulanır. Yetkisiz erişim suçunun konusu sebebiyle oluşan hafifletici hal düzenlemesi(*243/2*) ile karşılıksız yararlanma suçu arasında da özel-genel norm ilişkisi bulunduğundan, bu suçlar arasında da gerçek içtima uygulanır. Tez konusu suçların içtima yönünden değerlendirilmesi gereken esas suçlar; özel hayatın gizliliğini ihlal, kişisel verilerin hukuka aykırı olarak ele geçirilmesi, haberleşmenin gizliliğini ihlal, sistem engelleme bozma verileri yok etme veya değiştirme, bilişim sistemleri kullanılması suretiyle hırsızlık ve bilişim sistemleri aracılığıyla nitelikli dolandırıcılık suçlarıdır. Yetkisiz erişim suçu ve araya girme suçu yönünden içtima noktasında şartları mevcutsa fikri içtima uygulanmalı, aksi halde daima gerçek içtima uygulanmalıdır. Bileşik suçun oluşabileceği bir durum ise bu suçlar yönünden mevcut değildir.

Yetkisiz erişim suçunun temel halinde bir yıla kadar hapis veya adli para cezasına hükmedilir. Suçun konusu bedeli karşılığı yararlanılabilen sistemler olduğunda ise verilecek ceza yarı oranına kadar indirilecektir. Suçun neticesi sebebiyle ağırlaşmış halinde ise altı aydan iki yıla kadar hapis cezasına hükmolunur. Araya girme suçunun işlenmesi halinde ise bir yıldan üç yıla kadar hapis cezası verilecektir. Terörle Mücadele Kanunu md. 5'e göre yetkisiz erişim ve araya girme suçları terör amacı ile işlenmişse, verilecek hapis veya adli para cezaları yarı oranında artırılacaktır. Yetkisiz erişim suçunda hapis ve adli para cezası seçimlik olduğundan, her ikisine de beraber hükmedilemez. Yetkisiz erişim suçu yönünden kritik altyapılara ve araya girme suçu yönünden ise emniyet ve silahlı kuvvetler gibi kritik noktalara dair ağırlaştırıcı sebep düzenlemelerine gidilmesi mantıklı olacaktır. Tez konusu suçların işlenmesi halinde tüzel kişiler hakkında güvenlik tedbiri uygulanabilir. Bu suçlar ile bir tüzel kişi yararına haksız menfaat sağlanıyor ise TCK md. 60 gereğince iznin iptali ve/veya müsadere kararı tüzel kişilere yönelik de verilebilecektir.

KAYNAKÇA

AÇIKGÖZ Emre İkbal (2017), *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu*, Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara.

AKBULUT Berrin (2017), *Bilişim Alanında Suçlar*, İkinci Basım, Adalet, Ankara.

AKBULUT Berrin (2018), *Ceza Hukuku Genel Hükümler*, Beşinci Basım, Adalet, Ankara.

AKDENİZ Gökşin (2013), ‘’Hacker Etiği‘’, İçinde, *Hack Kültürü ve Hacktivizm,* ss. 9-16, Alternatif Bilişim, İstanbul.

AKÖZ Burak Cesur (2018), *Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları ile Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri*, Bilgi Teknolojileri ve İletişim Kurumu Bilişim Uzmanlığı Tezi, Ankara.

AKTAŞ Onur (2020), *Siber Güvenlik-Hacking Atölyesi*, Gazi Kitabevi, Ankara.

AKYILDIZ M. Alparslan ve SANER Doğukan (2020), *Web Sızma Testleri El Kitabı*, Gazi Kitabevi, Ankara.

ALTINOK Besim (2021), *Kablosuz Ağ Güvenliği(Saldırı-Savunma-Analiz),* Üçüncü Basım, Abaküs, İstanbul.

ALACA Bahattin (2008), *Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi(Antropolojik ve Hukuki Boyutları İle),* Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji(Sosyal Antropoloji) Anabilim Dalı Yüksek Lisans Tezi, Ankara.

Aljazeera, *India bought Israeli Pegasus spyware as part of weapons deal: NYT*, https://www.aljazeera.com/news/2022/1/29/india-bought-israeli-pegasus-spyware-as-part-of-weapon-deal-nyt, (ET: 03.03.2022).

AKINCI Hatice, ALIÇ A. Emre ve ER Cüneyd (2004), ‘’Türk Ceza Kanunu ve Bilişim Suçları‘’, İçinde, *İnternet ve Hukuk,* Derleyen: Yeşim M. Atamer, ss.157-277, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

ALP Barış Emre (2019), *Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu*, Adalet, Ankara.

APAYDIN Cengiz (2020), ‘’Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu‘’, *Terazi Hukuk Dergisi*, C. 15, S. 163, ss. 563-571.

APAYDIN Cengiz (2017), *Bilişim Suçları ve Bilişim Ceza Hukuku*, İstanbul.

APİŞ Özge (2018), ‘’Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri‘’, *Yasama Dergisi*, S. 37, ss. 49-86.

ARAALAN Cemal (2021), *Teknik ve Hukuki Boyutlarıyla Elektronik Ödeme Sistemlerinde Siber Güvenlik*, Seçkin, Ankara.

ASLAN YAVUZER Füsun (2020), *Nesnelerin İnterneti Uygulamalarının Güvenliği İçin Hafif Sikler Kriptografik Algoritmaların Analizi ve Güvenli Akıllı Bir Platform Uygulaması*, Trakya Üniversitesi Fen Bilişimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Doktora Tezi, Edirne.

AVŞAR Zeki ve ÖNGÖREN Gürsel (2010), *Bilişim Hukuku*, Türkiye Bankalar Birliği, İstanbul.

AYDOĞAN BOSCHELE Filiz ve ÇETİN ÖZTÜRK Özlem (2017), ‘’Dijital İletişim Teknolojileri ve Toplumsal Hareketler Bağlamında Hacktivizm‘’, *Üsküdar Üniversitesi Sosyal Bilimler Dergisi*, S.5, ss. 429-452.

BACAKSIZ Pınar ve YAĞMUR SÜMER Seda (2021), *Robotlar, Yapay Zeka ve Ceza Hukuku*, Adalet, Ankara.

BALCI Murat, ALŞAHİN M. Emin ve ÇAKIR Kerim (2021), *Ceza Muhakemesi Hukuku*, Adalet.

BARTLETT Jamie (2020), *Dark Net*, Çev: Yasin Konyalı, Timaş, İstanbul.

BAYRAKTAR Çiler Damla (2018), ‘’Ceza Muhakemesi Hukukunda Bir Koruma Tedbiri Olarak Otomatik Veri Taraması (Rasterfahndung): İnsan Hakları Bağlamında Bir Analiz‘’, *Ceza Hukuku Dergisi*, C. 13, S. 38, ss. 25-64.

BAYRAKTAR Köksal, KANGAL Zeynel T., EVİK Vesile Sonay, YILDIZ Ali Kemal, RETORNAZ Eylem Aksoy, BOZBAYINDIR Gülşah Bostancı, KARTAL Pınar Memiş, EVİK Ali Hakan, İNCEOĞLU Asuman Aytekin ve EROĞLU Fulya (2021), *Özel Ceza Hukuku C. VIII Ekonomi, Sanayi ve Ticarete İlişkin Suçlar-Bilişim Alanında Suçlar*, Onikilevha, İstanbul.

BBC, *Pegasus: Spyware Sold to Government's Targets Activist's,* https://www.bbc.com/news/technology-57881364, (ET: 03.03.2022).

Beyaz.net, *Black Box ve White Box Testi*, www.beyaz.net/tr/guvenlik/makaleler/black_box_ve_white_box_testi.html, (ET: 03.03.2022).

BİLEK Burak Tunç (2012), *Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri*, Gazi Üniversitesi Bilişim Enstitüsü Bilgisayar Eğitimi Anabilim Yüksek Lisans Tezi, Ankara.

BİLGEM (2017), *Güvenlik Yazılımı Tedariki Rehberi*

BİLGEM (2019), *Kablosuz Ağların İşletimi Rehberi*

BİLGEM (2020), *VOIP Rehberi*

BİLGEM (2020), *Alan Adı (Domain) Sistem Yönetimi Rehberi*,

BİLGEM (2021), *Sunucu Yönetimi Rehberi*

BİRTEK Fatih (2017), *Ceza Muhakemesinde Delil ve İspat*, Adalet, Ankara.

BRIDGES Dion Dalton (2020), *A Brief History of The…Cypherpunks*, Medium.org, https://medium.com/the-capital/a-brief-history-of-the-cypherpunks-31ae447a14f, (ET: 02.03.2022)

BÜYÜKÇAĞLAR Serkan (2013), *İnternet'te Sivil İtaatsizlik*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü İnsan Hakları Hukuku Yüksek Lisans Tezi, İstanbul.

CNBC, *JPMorgan and Other Banks Struck By Cyberattack*, https://www.cnbc.com/2014/08/27/fbi-probes-possible-hack-at-jpmorgan-report.html, (ET: 03.03.2022).

CENK Murat (2019), ''Siber Güvenlikte Kriptografi'', İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 2*, Ed. Şeref Sağıroğlu, Mustafa Şenol, ss. 63-82, Grafiker, Ankara.

Council of Europe (2022), *Germany-Cybercrime Legislation-Domestic Equivalent to the Provisions of the Budapest Convention*, https://rm.coe.int/octocom-legal-profile-germany/1680a5b48b, (ET: 20.04.2022).

Council of Europe, *Toplantı ve Dernek Kurma Hürriyetine Dair Taslak Rapor*, https://rm.coe.int/1680496a0b, (ET:02.03.2022).

Council of Europe (2008), *United States of America -Cybercrime Legislation-Country Profile*, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b9, (ET: 20.04.2022).

Cybercrime Convention Committee (2012), *T-CY Guide Note 1, On The Notion of ''ComputerSystem''*,rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMCo ntent?documentId=09000016802e79e6, (ET: 02.03.2022).

ÇEKİÇ Burak (2006), *İnternet Aracılığı ile İşlenen Suçlar,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Yüksek Lisans Tezi, İstanbul.

ÇETİN Muhammet Sefa (2021), ''Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu'', *TAAD*, C. 12, S. 45, ss. 1-28.

ÇOBAN Serhat (2020), ''Hackerlık Kavramı, Modeller ve Medyada Hackerlığın Sunumu'', *Bilişim Teknolojileri Online Dergisi*, C. 11, S. 40, ss. 43-64.

ÇÖLKESEN Toros Rifat (2018), *Network-TCP/IP-UNIX*, Onbirinci Basım, PapatyaBilim, İstanbul.

DARICILI Ali Burak (2017), ''Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi'', *ULİSA: Uluslararası Çalışmalar Dergisi Özel Sayısı*, C. 1, S. 1, ss. 1-24.

DARPA, ARPANET, https://www.darpa.mil/attachments/ARPANET_final.pdf, (ET:02.03.2022).

DEĞİRMENCİ Olgun (2019), ''Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi'', *Yaşar Hukuk Dergisi*, C. 1, S. 2, ss. 175-204.

DEMİR Bünyamin (2020), *Yazılım Güvenliği(Saldırı ve Savunma)*, Dikeyeksen, İstanbul.

DEMİRBAŞ Timur (2021), *Ceza Hukuku Genel Hükümler*, Seçkin, Ankara.

DEMİRCAN Tunç (2007), *Bilişim Alanında Suçlar*, Selçuk Üniversitesi Soyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Konya.

DEMİRKIRAN Pınar (2013), ''Hacktivizm'', İçinde, *Hack Kültürü ve Hacktivism*, ss. 27-34, Alternatif Bilişim, İstanbul.

Dijital Ceza Muhakemesi Hukuku, Ed. Bahri ÖZTÜRK, Durmuş TEZCAN ve Mustafa Ruhan ERDEM (2021), Seçkin, Ankara.

Dijital Türkiye Platformu (2021), *Dijitalleşme Yolunda Türkiye*, https://assets.kpmg/content/dam/kpmg/tr/pdf/2021/04/dijitallesme-yolunda-turkiye-raporu-2021.pdf, (ET: 01.03.2022).

DİJLE Hikmet ve DOĞAN Nurettin (2011), ‘’Türkiye’de Bilişim Suçlarına Eğitimli İnsanların Bakışı‘’, *Bilişim Teknolojileri Dergisi*, C. 4, S. 2, ss. 43-54.

DOĞAN Koray (2015), *Neticesi Sebebiyle Ağırlaşmış Suçlar*, Adalet, Ankara.

DOĞAN Ramazan (2014), *Bilişim Suçları*, Adalet, Ankara.

DOĞANAY Hamza Aytaç (2020), *Mobil Cihaz Adli Bilişiminde Karşılaşılan Güncel Zorluklar ve Delil Zinciri*, Legem, Ankara.

DOĞU Ali Haydar (2017), *Bilişim Hukuku*, Ekin, Bursa.

DÖNMEZER Sulhi ve ERMAN Sahir (2019), *Nazari ve Tatbiki Ceza Hukuku Cilt 2*, Ondördüncü Basım, DER, İstanbul.

DÜLGER Murat Volkan (2022), *Bilişim Suçları ve İnternet İletişim Hukuku*, Dokuzuncu Basım, Seçkin, Ankara.

DÜLGER Murat Volkan (2021), *Ceza Hukuku Genel Hükümler*, Hukuk Akademisi, İstanbul.

EKİCİ ŞAHİN Meral ve KORUCULU Irmak (2019), ‘’Bilişim Sistemine Girme Suçu-Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme‘’, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN’a Armağan*, C. 21, Özel Sayı, ss. 585-626.

EKİM Ahmet (2013), *Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi ve Raporlanması*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Gazetecilik Ana Bilim Dalı Yüksek Lisans Tezi, İstanbul.

ELBAHADIR Hamza (2021), *Hacking Interface*, Kodlab, Ankara.

ERDAĞ Ali İhsan (2010), ‘’Bilişim Alanında Suçlar(Türk ve Alman Ceza Hukukunda)‘’, *Gazi Üniversitesi Hukuk Fakültesi Dergisi* C. 14, S. 2, ss. 275-303.

ERDEM Merve ve ÖZOCAK Gürkan (2019), ‘’Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Hukukun Rolü‘’, *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* C. 68, S. 1, ss. 127-212.

ERDOĞAN Yavuz (2010), ‘’Bilişim Sistemine Girme ve Kalma Suçu‘’, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* C. 12, Özel Sayı, ss. 1363-1433.

EREN Ahu Karakurt (2020), ‘’Sızma testleri ile Türk Ceza Kanunu’nun 243, 244 ve 245/A Maddelerinde Düzenlenen Suçlar Arasındaki İlişkinin Değerlendirilmesi‘’, *Terazi Hukuk Dergisi,* C. 15, S. 164, ss. 747-764.

ERGÜN İsmail (2008), *Siber Suçların Cezalandırılması ve Türkiye’de Durum*, Adalet, Ankara.

ERMEYDAN Damla (2018), *Türk Ceza Kanunu’nda Bilişim Suçları*, Çağ Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Mersin.

EUROPOL, *Cybercrime,* www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime, (ET: 03.03.2022).

EUROPOL (2020), *Internet Organised Crime Threat Assesment,* https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf, (ET: 02.03.2022).

FBI, *Ransomware,* https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware, (ET: 10.11.2021).

Financial Times (2019), *WhatsAPP Voice Calls Used To İnject Israeli Spyware On Phones,* https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab, (ET: 03.03.2022).

GANGWAR Suraj ve NARANG Vinayak (2020), ‘’A Survey On Emerging Cyber Crimes and Their Impact Worldwide‘’, İçinde, *Encyclopedia of Criminal Activities and the Deep Web*, ss. 23-36, IGI Global, USA.

GERÇEKER Hasan (2020), *Yorumlu-Uygulamalı Türk Ceza Kanunu*, Seçkin, Ankara.

GÖKSOY Resul (2019), *Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması,* Seçkin, Ankara.

GÖKŞEN Elif (2014), *Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri*, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul.

GÜL Ahmet (2021), *Doğrudan Dolaylı Bilişim Suçları*, Seçkin, Ankara.

GÜL Yunus Emre (2021), *Savaş Hukuku 2.0 Siber Saldırılar ve Hukuk*, Hukuk Akademisi, İstanbul.

GÜLER Dilek (2018), ‘’Bilişim Sistemine Girme Suçu‘’, *KTO Karatay Hukuk Fakültesi Dergisi*, C. 3, S. 2, ss. 11-38.

GÜN Nagihan (2020), *Türk Ceza Hukukunda Bilişim Suçları,* Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara.

GÜRLER Fazıl (2013), *Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar,* Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara.

HABERTÜRK, *Mor Beyin Nedir,* https://www.haberturk.com/mor-beyin-nedir-mor-beyin-yazilimi-nedir-1772655, (ET: 03.03.2022).

HAFIZOĞULLARI Zeki ve ÖZEN Muharrem (2021), *Türk Ceza Hukuku Genel Hükümler*, USA, Ankara.

HAFIZOĞULLARI Zeki ve ÖZEN Muharrem (2012), *Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar*, Onüçüncü Basım, USA, Ankara.

HAKERİ Hakan (2021), *Ceza Hukuku Genel Hükümler*, Adalet, Ankara.

HANCI Hamit, TOKGÖZ Hilal ve YAPAR İshak (2018), ‘’Tıbbi Sistemleri ve Cihazları Hedef Alan Siber Saldırılar‘’, *Adli Bilimler Dergisi* C. 17, S. 1 ss. 32-39.

HEİNRİCH Bernd (2014), *Ceza Hukuku Genel Kısım 1*, Ed. Yener Ünver, Çev: Hakan Hakeri, Yener Ünver vd., Adalet, Ankara.

HENKOĞLU Türkay (2014), *Adli Bilişim-Dijital Delillerin Elde Edilmesi ve Analizi*, Pusula, İstanbul.

HİLGENDORF Eric (2021), ‘’Endüstri 4.0’da Sorumluluğun Erimesi ve Kendi Kendine Öğrenen Sistemler-Ceza Hukuku Açısından Sorun Özeti‘’, Çev. Enis Tiz, İçinde, *Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler*, ss. 47-61, Proje Yöneticisi. Kayıhan İçel, Ed. Yener Ünver, ss. 248-289, Seçkin, Ankara.

INTERPOL, *Cybercrime Operations,* https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations, (ET: 03.03.2022).

İHTİYAROĞLU Uğur (2020), ‘’Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi‘’, *Hacettepe Hukuk Fakültesi Dergisi*, C. 10, S. 2, ss. 406-440.

İLBAŞ Çığır (2009), *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi*, Başkent Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Ankara.

İTÜBİDB, Seyir Defteri, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/arp-(adres-%C3%A7%C3%B6z%C3%BCmleme-protokol%C3%BC), (ET: 03.03.2022).

KANGAL Zeynel T. (2021), *Yapay Zeka ve Ceza Hukuku*, Oniki Levha, İstanbul.

KARA Elif (2013), *Toplumsal Hareketlerin Dönüşümü ve Modern Bir Toplumsal Hareket Olarak Hacktivizm: Anonymous ve RedHack Örnekleri*, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Antalya.

KARA İlker (2015), ‘’Hacking (Yetkisiz Erişim) ve Hukuki Boyutu‘’, *Leges Hukuk Dergisi*, Kasım 2015, ss. 29-40.

KARABEY AKSAKALLI Işıl, ‘’Bulut Bilişimde Güvenlik Zafiyetleri, Tehditler ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi‘’, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, C. 5, S. 1, ss. 8-34.

KARACA Muhammet (2019), *Kritik Altyapılara Yönelik Bilişim Suçları; Türkiye ve AB Uygulamaları*, İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, İstanbul.

KARAGÜLMEZ Ali (2014), *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Beşinci Basım, Seçkin, Ankara.

KARAKEHYA Hakan (2009), ‘’Türk Ceza Kanunu’nda Bilişim Sistemine Girme Suçu‘’, *TBB Dergisi*, S. 81, ss. 1-24.

KARAKEHYA Hakan (2016), *Ceza Muhakemesi Hukuku*, Savaş, Ankara.

KAREEM Abdulrahman Hussein (2019), *Bilişim Suçları*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Konya.

Kaspersky Bilişim Teknolojileri Ansiklopedisi, Hack’in Kısa Tarihi, https://encyclopedia.kaspersky.com/knowledge/a-brief-history-of-hacking/, (ET: 02.03.222).

Kaspersky Bilişim Teknolojileri Ansiklopedisi, *Hacktivizm*, https://encyclopedia.kaspersky.com/glossary/hacktivism/, (ET: 02.03.2022).

Kaspersky, *What Is Rootkit- Definition and Explanation*, https://www.kaspersky.com/resource-center/definitions/what-is-rootkit, (ET: 03.03.2022).

KATOĞLU Tuğrul (2012), ‘’Ceza Hukukunda Suçun Mağduru Kavramının Sınırları‘’, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C. 61, S. 2, ss. 657-694.

KAYA Mehmet Bedii (2019), ‘’Hukuki Açıdan Bilişim Suçları-Siber Güvenlik ve Adli Bilişim‘’, İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 2*, ss. 213-279, Grafiker, Ankara.

KETİZMEN Muammer (2006), *Türk Ceza Hukuku'nda Bilişim Suçları*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Ankara.

KING Thomas C., AGGARWAL Nikita, TADDEO Mariarosaria ve FLORİDİ Luciano (2021), ‘’Yapay Zeka Suçu: Öngörülebilir Tehditleri ve Çözüm Yılları Üzerine Disiplinler Arası Bir Analiz‘’, Çeviren: Hasan Dursun, İçinde, *Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler*, Proje Yöneticisi. Kayıhan İçel, Ed. Yener Ünver, ss. 248-289, Seçkin, Ankara.

KILIÇ Ahmet (2018), ‘’Kaybolmuş veya Hata Sonucu Ele Geçmiş Eşya Üzerinde Tasarruf Suçu‘’, *Yıldırım Beyazıt Hukuk Dergisi*, C. 3, S. 2, ss.1-35.

KIZILARSLAN Damla (2019), *Haberleşmenin Gizliliğini İhlal Suçları*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul.

KOCA Mahmut ve ÜZÜLMEZ İlhan (2020), *Türk Ceza Hukuku Özel Hükümler*, Yedinci Basım, Adalet, Ankara.

KOCA Mahmut ve ÜZÜLMEZ İlhan (2021), *Türk Ceza Hukuku Genel Hükümler*, Ondördüncü Basım, Seçkin, Ankara.

KORUCU Onur (2021), *Veri Güvenliğinin İyileştirilmesi Sürecinde Küresel Standart, Çerçeve ve En İyi Uygulamaların Hukuki Uyuma Desteği*, Adalet, Ankara.

KÖKEN Enes (2021), ‘’Yapay Zekanın Cezai Sorumluluğu‘’, *Türkiye Adalet Akademisi Dergisi*, C. 12, S. 47, ss. 247-286.

KUNTER Nurullah, YENİSEY Feridun ve NUHOĞLU Ayşe (2013), *Açıklamalı Ceza Muhakemesi Kanunu Cilt 1*, Beta, İstanbul.

LAVRENOVS Arturs (2021), ‘’Towards Remediating DDoS Attacks, The NATO Cooperative Cyber Defence Centre of Excellence‘’, İçinde, *ICCWS 2021*, ss. 152-158, Talinn, Estonya.

LEINER Barry M., CERF Vinton G., CLARK David D., KAHN Robert E., KLEINROCK Leonard, LYNCH Daniel C., POSTEL Jon, ROBERTS Larry G. ve WOLF Stephen (1997), *Brief History of The Internet*, Internet Society.

ASS Açıklayıcı Raporu, https://rm.coe.int/16800cce5b, (ET: 04.01.2022).

MAHMUTOĞLU Fatih Selami, Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, C. 71, S. 1i, 2013, ss. 855-889.

MAHMUTOĞLU Fatih Selami ve KARADENİZ Serra (2017), *Türk Ceza Kanunu Genel Hükümler Şerhi*, Beta, İstanbul.

MALKOÇ İsmail (2013), *Açıklamalı Türk Ceza Kanunu Cilt 1*, Ankara.

MASUM Ersin ve SAMET Refik (2018), ‘’Mobil BOTNET ile DDoS Saldırısı‘’, *Bilişim Teknolojileri Dergisi,* C. 11, S. 2, , ss. 111-121.

M. Zekeriya (2013), *Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti,* Fırat Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Bilgisayar Eğitimi Anabilim Dalı Yüksek Lisans Tezi, Elazığ

New York Times, *JPMorgan and Other Banks Struck by Hacker*, https://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html, (ET: 03.03.2022).

New York Times, *F.B.I. Secretly Bought Israeli Spyware and Explored Hacking U.S. Phones,* https://www.nytimes.com/2022/01/28/world/middleeast/israel-pegasus-spyware.html, (ET: 03.03.2022).

OLLMANN Gunter (2007), *The Phishing Guide Understanding & Preventing Phishing Attacks.*

ORİYANO Sean Philip (2014), *Hacker Techniques, Tools, and Incident Handing,* Jones&Bartlett Learning, USA.

ORTA Mesut (2015), *Bilişim Suçlarında Adli Analiz*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, Konya.

ÖNDİN Hasan Burak (2017), *Türk Hukukunda Doğrudan Bilişim Suçları*, Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Eskişehir.

ÖZBEK Murat (2013), *Adli Bilişimde Delillerin Toplanması ve İncelenmesi,* İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Yüksek Lisans Programı Yüksek Lisans Tezi, İstanbul.

ÖZBEK Veli Özer (2010), *TCK İzmir Şerhi Türk Ceza Kanunu'nun Anlamı Cilt 1*, Onaltıncı Basım, Seçkin, Ankara.

ÖZBEK Veli Özer, DOĞAN Koray, BACAKSIZ Pınar ve TEPE İlker (2021a), *Türk Ceza Hukuku Özel Hükümler*, Onaltıncı Basım, Seçkin, Ankara.

ÖZBEK Veli Özer, DOĞAN Koray, BACAKSIZ Pınar ve TEPE İlker (2021b), *Türk Ceza Hukuku Genel Hükümler*, Seçkin, Ankara.

ÖZÇELİK Büşra (2019), *Bilişim Sistemine Girme Suçu,* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul.

ÖZEN Muharrem ve ÖZOCAK Gürkan (2015), ''Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)'', *Ankara Barosu Dergisi*, S. 1, ss. 43-77.

ÖZEN Mustafa (2017), *Ceza Hukuku Genel Hükümler Dersleri*, Adalet, Ankara.

ÖZENBAŞ Nazmiye (2012), *Neticesi Sebebiyle Ağırlaşmış Suçlarda Ceza Sorumluluğunun Esası,* Adalet, Ankara.

ÖZGENÇ İzzet (2005), *Türk Ceza Kanunu Gazi Şerhi(Genel Hükümler),* Seçkin, Ankara.

ÖZGENÇ İzzet (2021), *Türk Ceza Hukuku Genel Hükümler*, Onyedinci Basım, Seçkin, Ankara.

ÖZKAN İbrahim (2019), *Siber Saldırıların Ekonomik Boyutu*, Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü İktisat Anabilim Dalı Yüksek Lisans Tezi, Bilecik.

ÖZKÖSE Hasan (2014), *Makineler Arası Haberleşme (M2M) ve Türkiye İçin Düzenleyici Öneriler*, Bilgi Teknolojileri ve İletişim Kurumu Bilişim Uzmanlığı Tezi, Ankara.

ÖZMESTİK Fehmi Ünsal (2015), *Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı Yüksek Lisans Tezi, İstanbul.

ÖZSOY Nevzat (2019), ''Yargıtay Kararları Işığında Doğrudan Bilişim Suçları'', *Yaşar Hukuk Dergisi*, C. 1, S. 2, ss. 295-352.

ÖZTEKİN Alp (2021), *Türk İnternet Hukuku*, Seçkin, Ankara.

ÖZTÜRK Bahri ve ERDEM Mustafa Ruhan (2008), *Uygulamalı Ceza Muhakemesi Hukuku*, Seçkin, Ankara.

ÖZTÜRK Bahri ve ERDEM Mustafa Ruhan (2021), *Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku*, Seçkin, Ankara.

PALLI Hayati (2008), *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları,* Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Erciyes.

PARLAR Ali ve HATİPOĞLU Muzaffer (2010), *Türk Ceza Kanunu Yorumu Cilt 4,* Üçüncü Basım, Seçkin, Ankara.

PARLAR Ali ve ÖZTÜRK Mustafa (2020), *Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar*, Aristo, İstanbul.

POLAT Hüseyin (2014), ‘’Bilgisayar Ağları ve Adli Bilişim‘’, İçinde, *Adli Bilişim ve Elektronik Deliller,* Ed. Hüseyin Çakır, Mehmet Serkan Kılıç, Seçkin, Ankara.

POSTA, *Avusturya'ya saldıran Türk hacker bulundu' iddiası: 'General Osman' adıyla biliniyor,* http://www.posta.com.tr/avusturya-ya-saldiran-turk-hacker-bulundu-iddiasi-general-osman-adiyla-biliniyor-haberi-1272902, (ET: 03.03.2022).

RAY Donald ve LİGATTİ Jay, *Defining Injection Attacks Technical Report,* University of South Florida Department of Computer Science and Engineering, https://cse.usf.edu/~ligatti/papers/bronies.pdf, (ET: 03.03.2022).

SAĞIROĞLU Şeref (2018), ‘’Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler‘’, İçinde. *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 1, Siber Güvenlik ve Savunma-Farkındalık ve Caydırıcılık*, Ed. Şeref Sağıroğlu, Mustafa Alkan, ss. 21-45, Grafiker, Ankara.

SAĞIROĞLU Şeref (2019), ‘’Siber Güvenlik ve Ötesi‘’, İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 2, Siber Güvenlik ve Savunma-Problemler ve Çözümler*, Ed. Şeref Sağıroğlu, Mustafa Şenol, ss. 25-60, Grafiker, Ankara.

SAMET Refik ve ASLAN Ömer (2018), ‘’Kötü Amaçlı Yazılımlar ve Analizi‘’, İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 1*, ss. 225-255, Grafiker, Ankara.

SEMİZ Mustafa (2021), *Bilişim Suçları ve Soruşturma Yöntemleri*, Adalet, Ankara.

ŞENTÜRK Mustafa Yasir (2018), *Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinden Uygulanması*, Türk Hava Kurumu Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Ankara.

SARAN A. Nurdan (2019), ‘’Fidye Yazılımlar‘’, İçinde, *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 3,* Ed. Şeref Sağıroğlu, ss. 227-240, Grafiker, Ankara

SAYGILI Erhan (2018), *Web Uygulama Güvenliği-Hacking Yöntemleri*, Dikeyeksen, İstanbul.

Sorting Out The Difference Between M2M and IoT, https://blog.parker.com/site/usa/en-US/details-home-page/sorting-out-the-difference-between-m2m-and-iot-usi (ET: 01.03.2022).

SOYASLAN Doğan (2020a), *Türk Ceza Hukuku Genel Hükümler*, Dokuzuncu Basım, Yetkin, Ankara.

SOYASLAN Doğan (2020b), *Ceza Hukuku Özel Hükümler*, Onüçüncü Basım, Yetkin, Ankara.

SÖYLER Yasin (2013), *Kamu Hukuku Açısından İnternet İçeriğinin Düzenlenmesi ve Bu Alanda Devletin İdari Yaptırım Uygulama Yetkisi*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi, Ankara.

ŞAHBAZ İbrahim (2020), *Açıklamalı ve İçtihatlı Türk Ceza Kanunu Cilt 3*, Yetkin, Ankara.

ŞAHİN Cumhur (2019), *Ceza Muhakemesi Hukuku Cilt 1*, Seçkin, Ankara.

ŞEN Ersan (2008), *Telefon Dinleme, Gizli Soruşturmacı, X Muhbir*, Seçkin, Ankara.

ŞEN Semih Töner (2021), *Siber Uzay ve Uluslararası Hukuk*, Oniki Levha, İstanbul.

TANRIKULU Cengiz (2014), *Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi.

TARPLEY Philip ve JANSMA Steven D. (2016), *Autonomous Vehicles: The Legal Landscape In The US*, Norton Rose Fulbright, https://www.nortonrosefulbright.com/en/knowledge/publications/2951f5ce/autonomous-vehicles-the-legal-landscape-in-the-us, (ET: 03.03.2022).

TAŞKIN Cebrail (2018), *Ağ Teknolojileri ve Telekomünikasyon,* Pusula, İstanbul.

TAŞKIN Mustafa (2011), *Adli ve İstihbari Amaçlı İletişimin Denetlenmesi*, Seçkin, Ankara.

TAŞKIN Şaban Cankat (2008), *Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları,* Marmara Üniversitesi Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, İstanbul.

TDK Sözlük, https://sozluk.gov.tr, (ET: 01.03.2022).

TEKİN Eyüp (2017), *Adli Bilişimde Açık Kaynak Kullanımı*, Polis Akademisi Adli Bilimler Enstitüsü Kriminalistik Anabilim Dalı Yüksek Lisanst Tezi, Ankara.

TEPE İlker (2009), *Modern Ceza Hukuku Anlayışında İnternet Suçluluğu ve Türk Ceza Hukukundaki Yansımaları*, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Antalya.

TEZCAN Durmuş, ERDEM Mustafa Ruhan ve ÖNOK R. Murat (2021), *Teorik ve Pratik Ceza Özel Hukuku*, Ondokuzuncu Basım, Seçkin, Ankara.

THANGAMUTHU Poongodi, RATHEE Anu, PLANİMUTHU Suresh ve BALUSAMY Balamurugan (2020), ''Cybercrime'', İçinde, *Encyclopedia of Criminal Activities and the Deep Web*, ss. 1-23, IGI Global, USA.

The Evolution of Hacking, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/, (ET: 02.03.2022).

The NATO Cooperative Cyber Defence Centre of Excellence (2021), *Recent Cyber Events no: 12*, https://ccdcoe.org/uploads/2021/09/Report_The_Global_Threat_A4-1.pdf, (ET: 03.03.2022).

The New Hacker's Dictionary Version 4.2.2 (2012), Emereo Pty Limited.

Timothy C. (1994), *Kripto Anarşi ve Sanal Topluluklar* Mayıs, ABD, https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html, (ET:02.03.2022).

TOPALOĞLU Nurettin (2014), ''Bilgisayar Mimarisi'', İçinde, *Adli Bilişim ve Elektronik Deliller*, Ed. Hüseyin Çakır, Mehmet Serkan Kılıç, ss. 25-92, Seçkin, Ankara.

TOROSLU Nevzat ve TOROSLU Haluk (2021), *Ceza Hukuku Genel Kısım,* Savaş, Ankara.

TURAN Metin (2019), *Bilişim Hukuku*, Üçüncü Basım, Seçkin, Ankara, s. 49.

TÜRK Fatih (2019), *İstihbaratın Teşkilatlanma ve Yönetim Sorunsalı: A.B.D. Örneği*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı Yüksek Lisans Tezi, İstanbul.

Türk Standartları Enstitüsü (2014), *Sızma Testi Hizmeti Veren Personel ve Firmalar İçin Yetkilendirme Programı*.

T-CY (2013), *Guidance Note 2, Provisions of The Budapest Convention, Covering Botnets*,https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMCont ent?documentId=09000016802e7094, (ET: 05.03.2022).

UÇAR Hüdaverdi (2014), *5237 s. Türk Ceza Kanunu'nda Bilişim Suçları*, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara.

UKŞAL Mesut (2015), *Mobile Forensics*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul

ULUTAŞ Güzin (2019), ''Siber Güvenlik'', İçinde. *BGD Siber Güvenlik ve Savunma Kitap Serisi Cilt 2, Siber Güvenlik ve Savunma-Problemler ve Çözümler,* Ed. Şeref Sağıroğlu, Mustafa Şenol, ss. 87-101, Grafiker, Ankara.

USOM (2014a), *Akıllı Telefonlarda Güvenlik.*

USOM (2014b), *DDOS El Kitabı.*

USOM (2014c), *Siber Güvenliğe İlişkin Temel Bilgiler.*

USTA Gökhan (2019), *Ethical Hacking(Hacking Kursu)*, Seçkin, Ankara.

USTA Gökhan (2018), *Bilgisayar Ağlarında Saldırı ve Savunma*, Seçkin, Ankara.

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 Yüksek Lisans Tezi, İstanbul.

ÜNVER Yener (2003), *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, Seçkin, Ankara.

VAİSANEN Teemu, TRİNBERG Lorena ve PİSSANİDİS Nikolas (2016), *I Accidantally Malware – What Should I Do… Is This Dangerous*, The NATO *Cooperative Cyber Defence Centre of Excellence,* Talinn,

Wikipedia, *Backdoor*, https://en.wikipedia.org/wiki/Backdoor_(computing), (ET: 03.03.2022).

Wikipedia, *CPU Cache*, https://en.wikipedia.org/wiki/CPU_cache, (ET: 03.03.2022).

Wikipedia, *ECHELON*, https://en.wikipedia.org/wiki/ECHELON, (ET: 03.03.2022).

Wikipedia, *Internet of Things*, https://en.wikipedia.org/wiki/Internet_of_things, (ET: 03.03.2022).

Wikipedia, *İstemci*, https://tr.wikipedia.org/wiki/%C4%B0stemci, (ET: 03.03.2022).

Wikipedia, *Jargon File*, https://en.wikipedia.org/wiki/Jargon_File, (ET: 03.03.2022).

Wikipedia, *JP Morgan Chase Data Breach*, en.wikipedia.org/wiki/2014_JPMorgan_Chase_data_breach, (ET: 03.03.2022).

Wikipedia, *MAC Flooding*, https://en.wikipedia.org/wiki/MAC_flooding/, (ET: 03.03.2022).

Wikipedia, *M2M*, https://en.wikipedia.org/wiki/Machine_to_machine, (ET: 03.03.2022).

Wikipedia, *Network Virtualization*, https://en.wikipedia.org/wiki/Network_virtualization, (ET: 03.03.2022).

Wikipedia, *Raspberry Pi*, https://tr.wikipedia.org/wiki/Raspberry_Pi, (ET: 20.06.2022).

Wikipedia, *Sanallaştırma*, https://tr.wikipedia.org/wiki/Sanalla%C5%9Ft%C4%B1rma_(bili%C5%9Fim), (ET: 03.03.2022).

Wikipedia, *Sniffing Attack*, https://en.wikipedia.org/wiki/Sniffing_attack, (ET: 03.03.2022).

Wikipedia, *Smart Device*, https://en.wikipedia.org/wiki/Smart_device, (ET: 03.03.2022).

Wikipedia, *Sunucu*, https://tr.wikipedia.org/wiki/Sunucu_(bili%C5%9Fim), (ET: 03.03.2022).

Wikipedia, *Packet Analyzer*, https://en.wikipedia.org/wiki/Packet_analyzer, (ET: 03.03.2022).

Wikipedia, *PRISM*, https://en.wikipedia.org/wiki/PRISM_(surveillance_program), (ET: 03.03.2022).

Wikipedia, *Port*, https://en.wikipedia.org/wiki/Port_(computer_networking), (ET: 03.03.2022).

Wikipedia, *Rootkit*, https://en.wikipedia.org/wiki/Rootkit#cite_note-2, (ET: 03.03.2022).

Wikipedia, *Vulnerability*, https://en.wikipedia.org/wiki/Vulnerability_(computing), (ET: 03.03.2022).

YAYCI Esra (2007), *Bilişim Suçları*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara.

YENİDÜNYA Ahmet Caner (2005), ‘’Bilişim Sistemine Hukuka Aykırı Erişim Suçu‘’, *Legal Fikri ve Sınai Haklar Dergisi*, S. 4.

YERDELEN Erdal (2014), ‘’Mütemadi (Kesintisiz) Suç‘’, *TAAD*, C. 5, S. 18, ss. 113-152.

YETİM Servet, ‘’Siber Zorbalık-Türkiye ve ABD Karşılaştırması(ABD V. DREW DOSYASİ)‘’, *TBB Dergisi*, Yıl 2015, S. 120, ss. 325-385.

YURTCAN Erdener (2015), *Türk Ceza Kanunu Genel Hükümler Cilt 1*, TBB Yayınları, Ankara.

YÜKSEL Armağan Ebru Bozkurt (2021), ‘’Nesnelerin İnternetinin Hukuki Yönden İncelenmesi‘’, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, C. 17, S. 2, ss. 113-139.

ZAFER Hamide (2010), *Özel Hayatın Gizli Alanının Ceza Hukukuyla Korunması*, Beta, İstanbul.