MÜHF-HAD Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi • Cilt 29, Sayı 1, Haziran 2023, ISSN: 2529-0142, ss. 16-31 • DOI:10.33433/maruhad.1291371

ARAŞTIRMA MAKALESİ
RESEARCH ARTICLE

Türk Ceza Hukukunda Bilişim Sistemine Girme Suçuna İlişkin Değerlendirmeler (TCK.243/1)

Evaluations Regarding the Crime of Entering the Information System in Turkish Criminal Law

Pınar MEMİŞ KARTAL*, Gülfem IŞIKLAR ALPTEKİN**

ÖZ

Günümüzde bilişim sistemlerinin tanımlanması büyük önem kazanmıştır. Bunun en önemli sebebi, ortaya çıkabilecek hukuki sorunlara çözüm arayışında adil, hakkaniyete uygun bir sonuca ulaşabilmektir. Özellikle ceza hukuku yönünden yapılacak tartışmalarda bilişim sisteminin tanımlanması suçta ve cezada kanunilik bakımından büyük önem arz etmektedir. Bu nedenle bilişim sistemlerini tanımak aslen bilişim uzmanlarının görevidir ve her olayda mutlaka bu uzmanların teknik görüşüne başvurulmalıdır. Türk ceza hukukunda, Avrupa ülkelerinin çoğunda olduğu gibi bilişim sistemlerine karşı işlenen fiiller kanun içinde düzenlendikleri yerler farklı olsa da, suç olarak düzenlenmiştir. 5237 sayılı Türk Ceza Kanunu'nun 243. maddesinde düzenlenen bilişim sistemine girme, bilişim sisteminin güvenliğine ve bu sisteme duyulan güvene karşı işlenen bir suçtur. Bununla birlikte bir bilişim sisteminin tamamına ya da bir kısmına hukuka aykırı bir şekilde girilmesi durumunda veya bu ortamda kalınması halinde, bireyin özel hayatının gizliliği ve/veya haberleşme özgürlüğü de ihlal edilmektedir. Bu suçun öngörülme sebebinin, Türkiye'nin taraf olduğu Avrupa Konseyi Siber Suç Sözleşmesine taraf olmanın getirdiği yükümlülük olduğu düşünülebilir. Ancak, bu suçun Türk Ceza Kanunu'nda düzenlenmiş olmasındaki asıl amaç, günümüz teknolojilerinin kötüye kullanımı sonucu ortaya çıkabilecek ihlalleri engelleme amacıdır. Özet olarak, bu çalışmada, TCK.m.243/1 'de düzenlenen bilişim sistemine girme suçu incelenmiştir.

Anahtar Kelimeler: Bilişim Sistemi, Türk Ceza Kanunu, Sisteme Girme, Sistemde Kalma, Avrupa Konseyi Siber Suç Sözleşmesi.

ABSTRACT

Defining information systems has recently gained considerable importance. The main reason for this is to reach a fair and equitable outcome in the search for a solution to possible legal issues that may arise. The definition of the informatics system is of critical importance in terms of legality in crime and punishment, especially in discussions on Criminal Law. Therefore, it is primarily the duty of information technology experts to understand information systems, and in every case, it is essential to consult their technical opinion. In Turkish Criminal Law, as in most European countries, the acts committed against information systems are regulated as crimes, even if they are regulated in different parts of the law. Article 243 of the Turkish Penal Code No. 5237, which regulates enter to an information system, is a crime committed against the security of the information system and the trust in this system. However, in case of illegal access to all or part of an information system or staying in this environment, the privacy of the individuals, private life and/or freedom of communication is also violated. Although the reason for the anticipation of this crime can be said to be the obligation brought by being a party to the Council of Europe Cyber Crime Convention to which Turkey is a party, the purpose of the Turkish Penal Code No. 5237 is to prevent violations that may arise because of the misuse of today's technologies. In summary, this study will examine the crime of entering to an information system regulated in TPC Article 243/1.

Keywords: Information System, Turkish Penal Code, Entering to the System, Staying in the System, Council of Europe Cyber Crime Convention.

* Galatasaray Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi.
** Galatasaray Üniversitesi Bilgisayar Mühendisliği Bölümü Öğretim Üyesi.
Sorumlu Yazar/Correspondence Author: Pınar Memiş Kartal
E-posta/E-mail: pmemis@gsu.edu.tr
Geliş Tarihi/Received: 02.05.2023 **Kabul Tarihi/Accepted:** 17.05.2023

I. GENEL AÇIKLAMALAR

Bilişim sistemleri ve buna bağlı alanlar son yüzyılın en önemli konularının başında gelmektedir. Genel anlamda ekonomi, ulaşım, sağlık, eğitim gibi pek çok alanda bilişim sistemlerinin kullanılıyor olması, bu sistemlerin sıkı kontrol ve denetim altına alınması ihtiyacını yaratmıştır. Kişisel verilerin öneminin vurgulandığı[1] bu çağda bilişim sistemleri vasıtasıyla verilere en kısa sürede ve etkinlikte erişim hukukçuların da bu alana yoğunlaşmasına neden olmuştur. Türkiye'de de önemli bir araştırma alanı olan bilişim ve bununla bağlantılı ortaya çıkabilecek hukuki sorunlar, son yirmi yılın tartışma konularındandır.[2] Özellikle pandemi döneminde bilişim sistemleri vasıtasıyla pek çok alanda faaliyet gösterilebilmesi ile bilişim alanı ve bununla bağlantılı olarak yapay zekâ ve teknolojilerinin gücü ortaya çıkmıştır.

Bilişim sistemlerinin neredeyse tüm alanlarda, bireylere ve topluma hizmet maksadıyla kullanılmasının yanı sıra suç işlemek amacıyla kullanımı da oldukça yaygıdır. Teknolojik gelişimin bir parçası olan bilişim sistemlerinin suç işlemek maksadıyla kullanılmasının yanı sıra bizatihi bu sistemlerin kullanım amacıyla da bağlantılı olarak suçun konusunu oluşturduğu tespit edilmektedir. Bu sebeplerle Avrupa Konseyi'nin de konuya ilişkin çalışmaları Avrupa Siber Suç Sözleşmesi[3] ile şekillenmiş ve gerek 765 sayılı eski TCK'da, gerekse 5237 sayılı TCK'da bilişim suçları olarak ifade edilen suçlar düzenlenmiştir. Siber suç kavramının, bilişim suçlarından daha geniş bir kavram olduğu, *hakaret, cinsel taciz, dolandırıcılık gibi klasik birçok suç tipinin bilişim sistemleri aracılığıyla işlenmesini de kapsadığı* ifade edilmektedir.[4]

Bilişim sistemlerine yönelik işlenen suçlar ile bilişim sistemleri vasıtasıyla işlenen suçlar birbirinden farklıdır. Bilişim suçları olarak ifade edilen suçlar bilişim sistemlerine yönelik suçlar olup, bilişim sistemlerinin içinde yer alan verilere ilişkin olabileceği gibi, doğrudan bilişim sisteminin kendisini de hedef alabilmektedir.

Bu çeşitlilik geniş bir çalışma alanını oluşturduğundan çalışmada bilişim sistemine yönelik suçlardan sadece TCK.m.243/1'de düzenlenen "bilişim sistemine girme" suçu incelenecek, bu suçun gelişimi, unsurları ile yargı kararları değerlendirilecektir.

1 CONGER Sue/PRATT Joanne/LOCH Karen, Personal Information Privacy and Emerging Technologies, *Information Systems Journal*, Haziran 2012, https://doi.org/10.1111/j.1365-2575.2012.00402.x, erişim tarihi: 4 Nisan 2023.

2 KARAKEHYA Hakan, Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu, *Türkiye Barolar Birliği Dergisi*, Cilt: 22, Sayı: 81, Mart 2009, 189-191, (187-210)

3 23 Kasım 2001'de Budapeşte'de Devletlerin imzasına açılan Avrupa Konseyi Siber Suç Sözleşmesi, 1 Temmuz 2004'te yürürlüğe girmiş olup bu alandaki ilk uluslararası antlaşmadır. Türkiye bu Sözleşmeyi 10 Kasım 2010'da imzalayıp, 22 Nisan 2014 tarih ve 6533 sayılı Kanun ile onaylamıştır. Siber Suç Sözleşmesi ile ilgili ayrıntılı bilgi için bkz., KOCA Mahmut, Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku, Bilgi Toplumunda Hukuk, *Prof. Dr. Ünal Tekinalp'e Armağan,* Cilt III, 2003, 784; ÖNOK Murat, Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, *in: Prof.Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, Cilt 19, Sayı 2, Yıl:2013, 1241-1247; (ss.1229 – 1270).

4 ÖNOK, 1231.

A. BİLİŞİM SİSTEMİNE GİRME SUÇUNUN YASAL DAYANAĞI

Bilişim sistemine girme suçu başlığı altında düzenlenen hüküm 5237 sayılı TCK'nın 243. maddesinde şu şekilde düzenlenmiştir; "***Madde 243 – (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.***

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

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

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

TCK.m.243 düzenlemesinin, Avrupa Konseyi Siber Suç Sözleşmesinin 2.maddesinde düzenlenen "yasadışı erişim" ve 3.maddesinde yer alan "yasadışı araya girme" maddeleri dikkate alınarak kaleme alındığı[5] ve bu Sözleşmeye taraf olmanın gerektirdiği bir yükümlülüğün, bu Sözleşmeye daha taraf olmadan yerine getirildiği ifade edilebilecektir.

Bilişim sistemine girme veya orada kalma suçu olarak ifade edilen TCK.m.243/1 düzenlemesinde, 2016 yılında 6698 sayılı Kanunun 30. maddesi ile değişikliğe gidilerek "ve" bağlacı "veya" ile değiştirilerek suç tipi 2016 tarihindeki değişikliğe kadar "bilişim sistemine girme ve orada kalma" bundan sonra "bilişim sistemine girme veya orada kalma" olarak değişmiştir. Bu değişiklik elbette suçun uygulanma alanını genişletmiş ve bundan sonra bilişim sistemine hukuka uygun surette girmiş olsa bile kişi bu sistemde hukuka aykırı bir şekilde kalmaya devam ederse TCK.m.243/1'deki fiili meydana getirmiş kabul edilecektir. Bundan önce gerçekleşen eylemler bakımından bu değerlendirmeyi yapmak mümkün değildir.

Bilişim sistemine girme suçu 765 sayılı eski TCK'da öngörülmemiş bir suç tipidir. İlk defa 5237 sayılı TCK ile Kanun'a giren bilişim sistemine girme, TCK'nın ikinci kitabının, "Topluma Karşı Suçlar" başlıklı üçüncü kısmının, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde düzenlenen ve iki ayrı suçu öngören bir hükümdür.[6]

TCK.m.243'te düzenlenen suçlardan ilki bilişim sistemlerine girme veya orada kalma suçudur. Bu suçun oluşabilmesi için failin, bir bilişim sistemine, tamamına ya da bir kısmına hukuka aykırı olarak girmesi ya da hukuka uygun surette girse bile hukuka aykırı olarak orada kalması aranmaktadır.

TCK.m.243'te yer alan ikinci suç tipi ise maddenin son fıkrasında düzenlenen "veri nakillerini hukuka aykırı izleme"[7]dir[8]. Söz konusunu TCK.m.243. maddesinin 4. fıkrasında düzenlenen bu

5 YILDIZ Ali Kemal, Bilişim Sistemine Girme, *in: Özel Ceza Hukuku*, Cilt VIII, Oniki Levha, s. 231.

6 YILDIZ, s. 231.

7 KOCA Mahmut/ ÜZÜLMEZ İlhan, *Türk Ceza Hukuku Özel Hükümler*, Adalet, Ankara, 2022, 998 vd.

8 Verileri hukuka aykırı izleme ile ilgili karşılaştırmalı hukuk yönünden kısa değerlendirme için ayrıca bkz. SIEBER Ulrich,

hüküm yine Avrupa Konseyi Siber Suç Sözleşmesinin 3. maddesinde düzenlenen "Yasadışı Araya Girme" başlıklı hükmünün öngördüğü yükümlülüğün bir sonucudur.[9]

Çalışmamızın başlığı ve konusu bilişim sistemine girme olduğu için, burada TCK.m.243/4'te düzenlenen "veri nakillerini hukuka aykırı izleme suçu" incelenmeyecek, yeri geldiğinde kısaca değinilecektir.

B. KORUNAN HUKUKİ DEĞER

Bilişim sistemine girme suçu ile korunan hukuki değer öncelikle bilişim sisteminin güvenliğidir.[10] Bununla birlikte korunan hukuki değerin bilişim sisteminin güvenliği ve güvenilirliği olarak ifade edildiği[11] de tespit edilmektedir. Bu görüşleri destekleyen bir başka görüşe göre korunan hukuki değerin bilişim sisteminin güvenliği ve dokunulmazlığı olarak ifade ederken, bu hükümle bireylerin güvenli bir şekilde özgürce bilişim sistemlerini kullanmalarının amaçlandığı ifade edilmektedir.[12]

Bilişim sistemine girme suçu ile korunan hukuki değerin karma nitelikte olduğunu ifade eden doktrindeki bir görüşe göre, bu suçla birden fazla hukuki yararın korunduğunu ve bunların, *"bireylerin bilişim sistemleri içerisinde yer alan verileri, sırları ve özel hayatları yanında, bilişim sistemlerine hukuka aykırı girişler dolayısıyla verileri, sırları ve özel hayatları tehlikeye giren bireylerin bilişim sistemlerine olan güven"*[13] olduğu belirtilmektedir. Yine karma nitelikteki bir diğer görüş öncelikle bilişim sistemlerinin güvenliğinin korunduğunu; bununla birlikte özel hayatın gizliliği ile haberleşme özgürlüğünün de korunan hukuki değer olarak tespit etmektedir.[14] Bir başka görüş ise sistemin içindeki verilerin dışarıdan gelecek müdahalelere karşı korunduğu, özel hayatın gizliliği ile haberleşme özgürlüğünün korunduğunu ifade etmektedir.[15]

Kanaatimizce bilişim sistemlerine girme suçu ile korunan hukuki değer karma niteliktedir. Gerçekten de bilişim sistemine girme tek başına sadece sisteme dahil olmak anlamına gelmemekte, sisteme bir kere girdikten sonra verilere erişebilmek anlamına da gelmektedir. Nitekim kanun koyucu TCK.m.243/3'te verilerin yok olmasını da öngörmek suretiyle bu verilere erişimi kabul etmiştir.

Failin bilişim sistemine girdikten sonra kişinin özel hayatına ya da haberleşmesine ulaşıp ulaşamamasının bir önemi bulunmamaktadır. Erişme imkanının, olasılığının mümkün olması yeterlidir. Kanun koyucunun özel hayatın gizliliğini ya da haberleşmenin gizliliğini ihlal suçlarını düzenlerken koruduğu hukuki değer elbette bu haklardır ancak bilişim sistemine girme bu hakların

Bilişim Suçları, (çevirenler YENİSEY Feridun/ ZAİMOĞLU Damla); *in: Bilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku*, Seçkin, Ankara, 2021, s. 260-261.

9 KOCA/ÜZÜLMEZ, 998.

10 KOCA/ÜZÜLMEZ, 985.

11 DÜLGER Murat Volkan, *Bilişim Suçları ve İnternet, İletişim Hukuku*, Seçkin, Ankara, 2015, 348.

12 AKBULUT Berrin, *Bilişim Alanında Suçlar*, Adalet, Ankara, 2017, 118.

13 YILDIZ, 233.

14 TEZCAN Durmuş/ ERDEM Mustafa Ruhan/ ÖNOK Murat, *Teorik ve Pratik Ceza Özel Hukuku*, Seçkin, Ankara 2022, 1165.

15 YILMAZ Sacit, *Türk Ceza Hukuku Sisteminde Siber Suçlar*, Adalet, Ankara 2023, 194.

da ihlalini meydana getiren bir eylemdir. Dolayısıyla kanun koyucunun bilişim sistemine girme ile öncelikli olarak bilişim güvenliği ve bu sistemlere duyulan güveni koruduğu ifade edilebilecekse de kanaatimizce özel hayatı, kişisel verileri ve haberleşmenin gizliliğini de koruduğu ifade edilebilecektir.

II. SUÇUN UNSURLARI

A. MADDİ UNSUR

1. Fail

Bilişim sistemine girme suçunun faili herkes olabilir. Bu suçta fail bakımından bir özellik aranmamıştır. Bilişim sistemine girme suçunun bir tüzel kişi yararına işlenmesi durumunda ise, TCK.m.246 hükmü gereği, tüzel kişilere özgü güvenlik tedbiri uygulanacaktır. Bu suç yönünden tüzel kişilere özgü güvenlik tedbiri olarak özel bir düzenleme öngörülmediği için, bunlar hakkında uygulanacak hüküm güvenlik tedbirleri başlıklı 5237 sayılı TCK.'nın 60. maddesidir.

2. Mağdur

Bilişim sistemlerine girme suçunun mağduru yönünden görüş birliği bulunmamaktadır. Bir kısım yazar, mağdurda bir özellik bulunmadığını belirterek, bilişim sistemine girilen kişiyi suçun mağduru olarak kabul etmektedir.[16] Bir görüş de korunan öncelikli hukuki değer olarak bilişim sistemlerinin güvenliği olması nedeniyle bireylerin bu suçun mağduru olamayacaklarını ifade etmektedir.[17]

Kanaatimizce mağdur yönünden tespit ettiğimiz korunan hukuki değer çerçevesinde yorum yapacak olursak bilişim sistemine sahip olan kişilerin bu suçun mağduru olacağını ifade edebiliriz. Gerçekten de bilişim güvenliği ve bu sisteme duyulan güvenle birlikte özel hayatın gizliliği ve haberleşme özgürlüğü dikkate alınınca mağdurun herkes olabileceği sonucuna varılmaktadır.

3. Suç Konusu

Bilişim sistemine girme suçunun konusu, "bilişim sistemi" dir. Burada üzerinde durulması gereken husus bilişim sistemidir. Bilişim sistemi, insanlar, süreçler, teknolojiler ve verilerin bir araya gelerek bilgiyi düzenli ve anlamlı bir şekilde toplamak, işlemek, saklamak, yönetmek ve dağıtmak için birlikte çalıştığı bir yapıdır.[18] Bilişim, teknoloji alanındaki pek çok araç içerisinde ufak bir alanı kapladığı ifade edilse de yarattığı etki yönünden hiç tartışmasız ciddi hukuki sorunlar ortaya koymaktadır.[19]

Bilişim sisteminin temel amacı, bir organizasyon veya bireyin karar verme yeteneklerini, iletişimi, işbirliğini ve genel verimliliğini desteklemek ve geliştirmektir.[20] Bilişim sistemi hukukçuların

16 KOCA/ÜZÜLMEZ; 987; YILDIZ, 234; AKBULUT, 121.

17 TEZCAN/ERDEM/ÖNOK, 1165.

18 BOADEN R./LOCKETT G., Information Technology, Information Systems and Information Management: Definition and Development, *European Journal of Information Systems*, Cilt 1, Sayı 1, Yıl:1991, (23-32).

19 KÜZECİ Elif, Sayısal Fil, İnkılap, İstanbul, 2021, 42.

20 WOOD-HARPER A.Trevor/ANTILL Lyn/AVISON David Ernest, *Information Systems Definition: the Multiview Approach*, Blackwell Scientific Publications, United Kingdom 1985, (26-34).

tanımlayabilecekleri bir sistem değildir. Bu alanda tanım yapmaya, bu tanımlar arasındaki farkı ortaya koymaya yetkin kişiler, bilişim uzmanları, bilgisayar mühendisleri ve bu alanda ihtisas sahipleridir. Dolayısıyla hukukçuların yapmaları gereken tanımlanmış sistemlerin suçta ve cezada kanunilik ilkesi sınırları içerisinde kalarak değerlendirmeleridir.

Teknoloji ile hukuk; teknolojinin hukuka hem problemlerin çözümü için bir üretim alanı yaratması, hem de teknolojinin süreç yönetiminin kontrollü ve güvenilir olmasında hukukun desteğine ihtiyaç duyması açısından iki yönlü ve interaktif bir ilişki içindedir. Türkiye'de özellikle günlük şehir hayatında kullanılan bilişim sistemleri ile ilgili mevzuat, hizmetin yürütülmesi ile ilgili düzenlemelerden değil, kurumların yetki ve görevlerini tanımlayan düzenlemelerden oluşmaktadır. Bu durumun, görev ve yetki çatışmalarına ve kurumların ortak bir çalışma ortaya koyamamalarına sebep olduğu görülmektedir.[21]

Eggers ve Macmillan, 2015'te "Kamunun Geleceğine Yolculuk" başlıklı raporlarında, dijital devrimin dört temel teknolojinin kesişim alanından meydana geldiğini vurgulamışlardır. [22] Bu bahsedilen teknolojiler sosyal, mobil, analitik ve bulut teknolojileridir. Giyilebilir teknolojiler ve mobil cihazların kullanımı yaygınlaşıp, insanları ve nesneleri her an bağlantılı bir hale getirmiştir. Rapora göre, dijitalleşme ile birlikte kamu hizmeti anlayışında da köklü değişiklikler gerçekleşmiştir. Özellikle 2020 itibariyle dijitalleşmeye bağlı değişimler başlamıştır. İnsansız hava araçları, suçlu analiz uygulamaları, mobil-sanal kelepçe uygulamaları gibi uygulamaların gelişmesi ile hukuk alanında dijital dönüşüm devam etmektedir. Ulaşım alanında dijital sinyallere dayalı toplu ulaşım sistemleri, sürücüsüz otomobiller, self – servis havaalanları, mobil cihaz destekli ulaşım sistemleri, elektrikli scooterlar, hukuksal çerçeveye oturtulması gereken başlıklar arasında yer almaktadır.[23]

Sonuç olarak, suçun konusu olarak genel bir biçimde ifade edilen bilişim sistemleri artık bilgisayar, bilişim ya da internet ile ifade edilmemektedir. Suçun konusu bilişim uzmanları olmaksızın tespit edilemeyecek ciddi bir uzmanlık alanı haline gelmiştir.

4. Hareket

Bilişim sistemlerine girme suçu TCK.m.243/1'de düzenlenmiştir. Madde başlığı fıkra düzenlemesinde öngörülen suçu karşılasa da aslında 4 fıkradan oluşan düzenlemeden iki farklı suç öngörüldüğüne yukarıda değinilmiş ve çalışmamızın sadece TCK.m.243/1'i kapsadığı ifade edilmiştir. Bu gerekçelerle madde başlığının düzenlemeyi kapsamadığı tespit edilmektedir.

Bilişim sistemine girme suçu düzenlemesinde, 24 Mart 2016 yılında 6698 sayılı Kanunun 30. maddesi ile değişikliğe gidilerek "ve" bağlacı "veya" ile değiştirilmiştir. Böylelikle söz konusu suç tipi

21 GÖÇOĞLU Volkan, *Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine Bir İnceleme,* MANAS Sosyal Araştırmalar Dergisi, Cilt 9, Sayı 1, Yıl: 2020, (615-628).

22 EGGERS William D./MACMILLAN, Paul, *KAMU 2020: Kamunun Geleceğine Yolculuk*, Deloitte, s. 6-8, 2015. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/tr-kamu%202020-kamunun %20gelecegine%20yolculuk.pdf, erişim tarihi: 6 Nisan 2023.

23 GÖÇOĞLU, 616.

2016 tarihindeki değişikliğe kadar "bilişim sistemine girme ve orada kalma" iken, bu tarihten sonra "bilişim sistemine girme veya orada kalma" olarak değişmiştir. Bu değişiklik elbette suçun uygulanma alanını genişletmiş ve bundan sonra bilişim sistemine hukuka uygun surette girmiş olsa bile kişi bu sistemde hukuka aykırı bir şekilde kalmaya devam ederse TCK.m.243/1'deki fiili meydana getirmiş kabul edilecektir. Bundan önce gerçekleşen eylemler bakımından bu değerlendirmeyi yapmak mümkün değildir.[24] Gerçekten de eski halindeki "ve" bağlacı ile eylem bağlı hareketli bir suç şeklinde düzenlenmek suretiyle, suçun meydana gelmesi için her iki hareketin gerçekleşmesi aranmaktayken değişiklikle fiil seçimlik hareketli suç haline gelmiştir.

TCK.m.243/1 düzenlemesine göre, suçun hareket unsuru bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme veya orada kalmaktır. Burada fail hukuka aykırı bir şekilde bilişim sistemine girecek veya hukuka aykırı ya da hukuka uygun girdiği sistemde hukuka aykırı olarak kalması gerekecektir.

Kanun koyucunun seçimlik hareketli suç olarak düzenlediği bilişim sistemine girmede seçimlik hareketler, hukuka aykırı bir şekilde bilişim sisteminin bütününe veya bir kısmına girme veya orada kalmaktır. Sisteme girip kalmaya devam eden failin eylemi tek fiil olarak kabul edilecektir. Bir başka ifadeyle seçimlik hareketlerin ikisinin birden gerçekleşmiş olması eylemi birden fazla suç haline getirmez, yine tek bir fiil söz konusu olur. Ancak burada dikkat edilmesi gereken husus, bir bilişim sistemine girme ve o sistemde kalma halinde seçimlik hareketlerin tek fiil oluşturacağıdır, [25] hareketlerin farklı sistemler üzerinde gerçekleşmesi halinde ise tek suçtan söz edilemeyeceği açıktır.

Seçimlik iki hareket de serbest hareketli olup, bunlardan bilişim sistemine girme icra-i niteliktedirler. Diğer seçimlik hareket olan bilişim sistemi ortamında kalmaya devam etmek ise kanaatimizce ihmali niteliktedir. Ortamda kalmaya devam etmek pasif bir davranışı gerektirdiğinden artık burada failin sistemden çıkma konusunda iradi bir ihmali olduğu tespit edilmektedir.

a. Bilişim Sisteminin Bütününe veya Bir Kısmına Hukuka Aykırı Olarak Girme

Bilişim sistemine girme suçunun ilk seçimlik hareketi olarak bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme hareketinin bu suçu oluşturabilmesi için sistemin bütününe ya da bir kısmına hukuka aykırı bir şekilde girilmiş olması gerekir.

Bilişim sistemine hukuka aykırı olarak girmekten maksadın fiziki bir şekilde olmaksızın, *bilişim sistemlerinin soyut alanına girmek* olarak ifade edilmektedir.[26]

Bir başka hukuki tanıma göre ise, sisteme girmekten maksat, *sistem güvenliğini devre dışı bırakmak suretiyle sistemin tamamına veya bir bölümüne erişmek*tir.[27] *Bilişim sisteminde bulunan verilere*

24 TEZCAN/ERDEM/ÖNOK, 1167; APİŞ Özge, Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama, Elkoyma Koruma Tedbirleri, in: *Yasama Dergisi*, Cilt: 13, Sayı:37, Haziran 2018, 52, (49-86).

25 AKBULUT, 126.

26 KOCA/ÜZÜLMEZ, 990; APİŞ, 62; DÜLGER, 363.

27 TEZCAN/ERDEM/ÖNOK, 1167.

ulaşma ve müdahale imkânı bulunduğu anda sisteme girme işleminin gerçekleştiğinin kabulünün gerekli olduğu da ifade edilmektedir.[28]

Doktrinde bir başka görüş ise bilişim sistemine girmek yerine, bu sisteme erişmek ifadesinin kullanılması gerektiğini; girmek eyleminin fiziksel bir alana girmeyi çağrıştırdığından erişim kavramının daha doğru olduğu bir terim tercihi olduğunu ifade etmektedir.[29]

Bilişim sistemine hukuka aykırı girmekten maksat, bilişim sistemi sahibinin rızası olmaksızın girmektir. Rızanın olduğu halde, fiil hukuka aykırı olmayacağından suç da oluşmayacaktır.

Bilişim sistemine hukuka aykırı bir şekilde girmek yeterlidir, sistemde bulunan verilere erişmiş olmanın, suçun gerçekleşmesi yönünden bir önemi bulunmamaktadır. Ancak veriye erişimin bu suç açısından önemi, söz konusu fiil nedeniyle sistemin içerdiği veriler yok olması veya değişmesi halinde, TCK.m.243/3'te daha ağır yaptırım öngörülmüş olmasıdır. Bununla birlikte verilerin verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren failin fiilleri TCK.m.244/2 yönünden de değerlendirilecektir. Bu hükümler birbirleri ile karıştırılma ihtimali dolayısıyla tartışılmakta ve eleştirilmektedir.[30]

Doktrinde başkası adına zimmetli olan bilgisayarlara "işlerin yürütülmesi amacıyla" girilmesi durumunda TCK.m.243'ün oluşmayacağı ifade edilmektedir.[31] Kanaatimizce burada her münferit olayı ayrı değerlendirmek ve suçun oluşup oluşmadığını tespit etmek gereklidir.

Bilişim sisteminin tamamına ya da bir kısmına girme, yukarıda da ifade edildiği üzere, icra-i nitelikte ve serbest hareketlidir.

Bilişim sistemine girme suçunda sisteme girme eylemi sistemin bütününe girme şeklinde olabileceği gibi bir kısmına girme de suçu meydana getirir. Sistemin tamamına ya da bir kısmına girildiğinin tespiti konunun uzmanı kişiler tarafından gerçekleştirilir.

b. Bilişim Sisteminde Hukuka Aykırı Bir Şekilde Kalmaya Devam Etme

Bilişim sisteminde hukuka aykırı bir şekilde kalmaya devam etme de bu suçun ikinci seçimlik hareketidir. Fail bilişim sistemine girmeden bu ortamda kalmaya devam edemeyeceğinden aslında bu hareket yönünden bilişim sistemine girme ile bağlı bir hareket olduğu ifade edilebilir. Burada fail, bilişim sistemine hukuka aykırı bir şekilde girmiş olabileceği gibi, sisteme hukuka uygun olarak da girmiş olabilir, söz konusu ikinci seçimlik hareketin TCK bakımından suçu meydana getiren hareket olabilmesi için sistemde kalmaya devam etmenin hukuka aykırı olarak gerçekleşmesi gereklidir.

28 YILDIZ, 238.

29 ÖZBEK Veli Özer/ DOĞAN Koray/ BACAKSIZ Pınar, *Türk Ceza Hukuku Özel Hükümler*, Seçkin, Ankara 2022, 986.

30 ÖZBEK/DOĞAN/BACAKSIZ, 988.

31 EKİCİ ŞAHİN Meral/ KORUCULU Irmak, Bilişim Sistemine Girme Suçu-Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarda İşlenmesine İlişkin Bir Değerlendirme, in: *DEHFD*, *Prof.Dr. Durmuş Tezcan'a Armağan, Özel Sayı, Cilt I;* İzmir 2019, 598 vd. ; TEZCAN/ERDEM/ÖNOK, 1168.

Sisteme hukuka aykırı bir şekilde girdikten sonra orada kalmaya devam eden fail, bu hükümde öngörülen iki seçimlik hareketi gerçekleştirmiş olsa da tek suç gerçekleşmiş olacaktır.[32]
Bilişim sisteminde hukuka aykırı bir şekilde kalmaya devam etme ihmali bir suçtur.

5. Netice

Bilişim sistemine girme, neticesi harekete bitişik bir suçtur. Bu suça sırf hareket suçu da denilmektedir.[33] Bu tip suçlarda nedensellik bağı bakımından bir tartışma da bulunmamaktadır.

Bu suçta zarar neticesi aranmadığı gibi, kanun koyucu zarar doğma ihtimalini de dikkate almadığından fiil soyut tehlike suçudur.[34]

6. Teşebbüs

Bilişim sistemine girme suçu neticesi harekete bitişik bir suçtur. Ancak hareketle neticenin ayrılabildiği durumlarda teşebbüs söz konusu olabilir. Bilişim sistemine girme teşebbüse elverişlidir, fail kendi elinde olmayan bir sebeple sisteme girmeyi başaramazsa teşebbüs söz konusu olacaktır.[35]

Bilişim sistemi ortamında hukuka aykırı bir şekilde kalmaya devam etme ise teşebbüse elverişli değildir.[36] Hukuka uygun bir şekilde sisteme girdikten sonra hukuka aykırı olarak sistemde kalmaya devam etmek de teşebbüse elverişli değildir. Bir kere sisteme girildikten sonra kalmanın gerçekleşmemesi failin çıkma iradesi ve/veya sistemin iznine bağlıdır. Girme fiilini takip eden fiil kalma eylemidir, dolayısıyla teşebbüs bu hareket yönünden meydana gelmesi mümkün olmayan bir özel görünüm biçimidir.

B. MANEVİ UNSUR

Bilişim sistemine girme suçu kasten işlenebilen bir suçtur. Genel kast yeterlidir, failin suçu işleme amacı dikkate alınmamıştır.[37] Bilişim sistemine girme taksirle işlenebilen bir suç değildir, kanun koyucu bu suçun taksirli halini öngörmemiştir. Dolayısıyla internette gezinirken dikkatsizlik ve özensizlikle bir sisteme giren kişinin eylemi manevi unsuru bulunmadığından suç teşkil etmeyecektir.[38]

Suçun olası kastla işlenip işlenmeyeceği tartışılmıştır.[39] Bilişim sistemlerine girme suçunun olası kastla işlenmesi mümkündür.[40] Burada TCK m. 21 kapsamında öngörülen olası kast uygulama alanı

32 KOCA/ÜZÜLMEZ, 992.

33 TEZCAN/ERDEM/ÖNOK, 1169; YILDIZ, 242.

34 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.1, YIL 2013, 861.

35 AKBULUT, 150.

36 AKBULUT, 151.

37 TEZCAN/ERDEM/ÖNOK, 1171; KARAKEHYA, 201.

38 KARAKEHYA, 201.

39 KOCA/ÜZÜLMEZ, 993; YILDIZ, 244; AKBULUT, 139; EKİCİ/KORUCULU, 609-610; aksi görüş TEZCAN/ERDEM/ÖNOK, 1172; ÖZBEK/DOĞAN/BACAKSIZ, 990.

40 TEZCAN/ERDEM/ÖNOK, 1172; ÖZBEK/DOĞAN/BACAKSIZ, 990.

bulabilecektir. Buna mukabil bilişim sistemine girmenin ancak doğrudan kastla işlenebileceği için olası kasta elverişli olmadığı da belirtilmektedir.[41]

C. HUKUKA AYKIRILIK UNSURU

Bilişim sistemlerine girme hukuka aykırı bir şekilde gerçekleştiği takdirde suç teşkil edecektir. Kanun koyucu bu suçun gerçekleşebilmesi için, hukuka özel aykırılık halini aramış ve fiil hukuka uygun bir şekilde gerçekleştiriliyorsa bunun suç teşkil etmeyeceğini ifade etmiştir. Bilişim sistemine girme veya orada kalma fiillerinin suç teşkil etmemesi için ilginin geçerli rızasının bulunması (TCK.m.26/2) ya da kanun hükmü gereği (TCK.m.24/1) bilişim sistemine girmenin hukuka uygun kabul edilmesi gerekmektedir.[42]

Rızanın hukuka uygunluk sebebi olarak kabul edilebilmesi için TCK.m.26/2'nin koşullarının oluşması gerekmektedir. Buna göre, kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez. Bu rızanın hukuken geçerli olabilmesi için ilginin rızasının serbest olması, rızanın hür bir şekilde açık ya da zımni olarak ifade edilmesi gereklidir. Üzerinde baskı kurulmuş, cebir, tehdit ile alınmış rıza hukuka uygunluk sebebi olarak değerlendirilmeyecek, eylem suç teşkil edecektir.

Kanun hükmünün yerine getirildiği durumlarda da bilişim sistemine girme suç oluşturmayacaktır. Ancak burada da kanun hükmünün öngördüğü sınırlara uyulması gerekmektedir. Aksi halde şartları oluştuysa ceza sorumluluğunu kaldıran ya da azaltan sebeplerde sınırın aşılması başlığını taşıyan TCK.m.27. madde hükmü uygulanacak ya da şartları dahi oluşmamışsa fiil hukuka aykırı olacağından suç oluşmuş denilecektir. Kanunun hükmünün hukuka uygunluk sebebi olarak suç tipine ilişkin örnek düzenleme 5271 sayılı CMK.m.134 verilebilir.[43]

D. SUÇU ETKİLEYEN NEDENLER

Bir bilişim sistemine hukuka aykırı olarak girme veya ortamda kalma fiili bakımından suçu etkileyen hafifletici sebep TCK.m.243/2'de düzenlenmiştir. Buna göre; bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kişinin, bu fiillerini bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi durumunda hakkında verilecek ceza yarı oranına kadar indirilir. Bu düzenleme belli bir bedel karşılığı yararlanılan sistemlere izinsiz girilmesi ve burada kalınması halini öngörmektedir. Doktrinde bu düzenlemenin yerinde bir düzenleme olduğu ifade edilerek, bir bedel ödenmeksizin kullanılan sisteme girmenin daha ağır sonuçları olduğu belirtilmektedir.[44]

Suça etki eden ve ağırlaştırıcı sebep olarak düzenlenen bir diğer sebep ise TCK'da değil, 3713 sayılı Terörle Mücadele Kanununda yer almaktadır.[45] Terörle Mücadele Kanununun 4. maddesine göre, TCK.m.243'ün terör amacıyla işlenmesi halinde terör suçu sayılacağı belirtilmiştir.

41 KOCA/ÜZÜLMEZ, 993; YILDIZ, 244; AKBULUT, 139; EKİCİ/KORUCULU, 609-610.

42 YILDIZ, 245.

43 ÖZBEK/DOĞAN/BACAKSIZ, 990; YILDIZ, 245; APİŞ, 67 vd.

44 KOCA/ÜZÜLMEZ, 994.

45 YILDIZ, 245.

E. NETİCESİ SEBEBİYLE AĞIRLAŞMIŞ HAL

Bilişim sistemlerine girme suçu bakımından TCK.m.243/3'te netice sebebiyle ağırlaşmış hal düzenlenmiştir. Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse TCK.m.243/1'de öngörülenden daha ağır ve farklı bir netice meydana gelmiş olacaktır. Ancak meydana gelen bu netice yönünden failin buna yönelik kastının bulunmaması gerekir.[46] Burada failin öngörmesi gereken, fakat öngörmediği bir neticeden dolayı sorumluluk meydana gelmektedir (TCK.m.23).

Failin meydana gelen bu ağır neticeye yönelik kastının varlığı kabul edildiği takdirde fiil artık TCK.m.243 değil TCK.m.244 kapsamında değerlendirilecektir. Bu nedenle doktrinde de her iki fiilin birbiri ile karıştırılması ihtimaline dikkat çekilmek suretiyle eleştirilmiştir.[47]

III. SUÇLARIN BİRLEŞMESİ VE İŞTİRAK

A. SUÇLARIN BİRLEŞMESİ

Bilişim sistemlerine girme suçu seçimlik hareketli bir suç olması nedeniyle, failin kanunda yer alan hareketlerin birini ya da hepsini gerçekleştirmiş olması fark etmeyecek, tek bir suç meydana geldiği için buna göre değerlendirme yapılacaktır.

Bilişim sistemlerinde hukuka aykırı olarak kalmaya devam etme kesintisiz bir suçtur. Burada kalmaya devam ettiği sürece tek bir suç vardır.[48]

Failin bilişim aynı bilişim sistemine belirli zaman aralıklarıyla, birden fazla kere aynı suç işleme kararı icrası kapsamında girmesi halinde TCK.m.43'teki zincirleme suç hükümleri uygulanacaktır. Yargıtay 12. Ceza Dairesinin suçun sübutu ile zincirleme suça dikkat çektiği kararında aktarılan olay şu şekilde gerçekleşmiştir: *"Sanığın, duruşmada doğruluğunu kabul ettiği Cumhuriyet Başsavcılığınca alınan; "... ..... adına açılmış sahte profil hesabını da benim açtığım doğrudur; ancak ben buradan hiç bir şekilde paylaşımda bulunmadım. Kendisi adına herhangi bir yazışma yapmadım... Benim kendisine ait bilgileri fotoğrafları twitter ve facebook adreslerine izinsiz girmem elde etmem söz konusu olamaz. Çünkü o dönemde tam bir bilgisi olmadığı için bana bu adreslerinin mail bölümlerinin şifrelerini kendisi vermiştir. Ben bu şifreleri kullanarak onun bilgisi dahilinde zaten giriyordum. Fotoğraflarını ise facebook adresinden herkes zaten görebilir; ancak, onun twitter hesabına girip de onun adına yazılar yazmam doğru değildir. Ancak bir facebook hesabı açtığım doğrudur; ama, dediğim gibi bu hesaptan resimlerine veya bilgilerine girerek arkadaşlarıyla konuştuğum doğru değildir... arkadaşlığımız bittiğinden itibaren kendisi benim bildiğim şifreleri değiştirmiştir, benim şu an için bu mail adreslerine veya onun hesaplarına girmem mümkün değildir..." biçimindeki 06.07.2012 tarihli ifadesi ve duruşmanın 20.02.2013 tarihli oturumunda alınan "... twitter şifresini bana kendisi vermiştir... twitter hesabına bir kez kendisinin yanında girdim, başkaca bu hesabı kullanmadım ve şifresini de değiştirmedim..." şeklindeki savunması karşısında, mağdurun beyanları, sahte facebook ile twitter hesabına*

46 TEZCAN/ERDEM/ÖNOK, 1170.

47 KOCA/ÜZÜLMEZ, 995.

48 YILDIZ, 247.

ilişkin belge örnekleri ve dosyada mevcut diğer deliller birlikte değerlendirilerek, iddianamede verileri hukuka aykırı olarak verme veya ele geçirme, sistemi engelleme, bozma, verileri yok etme veya değiştirme olarak nitelendirilen suçların yanı sıra iddianamedeki anlatıma ve mevcut delil durumuna nazaran TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme ile TCK'nın 132/1. madde ve fıkrasındaki haberleşmenin gizliliğini ihlal suçlarının da sübutuna ilişkin kanıtlar tartışılıp, sanığa isnat edilen eylem ve/veya eylemlerin sübut bulduğu sonucuna varıldığı takdirde, sübutu kabul edilen her bir eylemin hangi tarihte işlendiği ve TCK'nın 43/1. madde ve fıkrasındaki zincirleme suç koşullarının oluşup oluşmadığı denetime olanak verecek şekilde gerekçelendirilerek, sanığın hukuki durumunun takdir ve tayini gerekirken, yasal ve yeterli olmayan yazılı gerekçelerle verileri hukuka aykırı olarak verme veya ele geçirme ile zincirleme şekilde sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarından ayrı ayrı mahkumiyet hükümleri kurulması," (Yargıtay 12. CD, E. 2019/10291, K. 2020/6962, T. 9.12.2020)[49].

Fikri içtimaın da meydana gelebileceği, tek fiille birden fazla hükmün ihlal edilebileceğinin de mümkün olduğu belirtilmektedir (TCK.m.44).[50] Buna göre sisteme giren bir kimse aynı zamanda açık olan özel hayata ilişkin bir veriyi de okuma imkanına erişiyorsa artık fikri içtimaın olacağını ve daha ağır cezası olan TCK.m.134'ün uygulanacağı belirtilmektedir. Bilişim sistemine girme ile aynı zamanda, doğrudan özel hayata ya da haberleşme verilerine erişimin ikinci bir fiil olmadan mümkün olamayacağı için, fikri içtimaın gerçekleşmesi çok güçtür.

Bilişim sistemine girildikten sonra TCK.m.244'te yer alan düzenlemede öngörüldüğü gibi, bir bilişim sisteminin işleyişinin engellenmesi veya bozulması (TCK.m.244/1) veya bir bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verileri başka bir yere gönderilmesi (TCK.m.244/2) ya da belirtilen bu fiilleri bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinden işlenmesi halinde tüketen – tüketilen norm ilişkisinin meydana gelecek ve artık bilişim sistemine girme (TCK.m.243) değil, TCK.m.244 uygulanacaktır.[51]

B. İŞTİRAK

Bilişim sistemlerine girme suçu, iştirakte özellik arz etmez. Özgü bir suç olmadığı için bu anlamda bunlara ilişkin kurallar da uygulanmaz, iştirake ilişkin genel düzenlemeler uygulanır.

IV. YAPTIRIM VE YARGILAMA

A. YAPTIRIM

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. Bu fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. Söz

49 Yargıtay 12. CD. Kararı için bkz., https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=12cd-2019-10291.htm&kw=Bili%C5%9Fim+sistemine+girme+su%C3%A7u&cr=yargitay#fm, erişim tarihi: 10.02.2023.

50 KARAKEHYA, 207.

51 TEZCAN/ERDEM/ÖNOK, 1176.1

konusu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Bilişim sistemine girme suçu bir tüzel kişi yararına işlenirse, TCK.m.60 çerçevesinde bu tüzel kişi hakkında güvenlik tedbirine hükmolunur.

B. YARGILAMA

Bilişim sistemlerine girme re'sen kovuşturulan bir suçtur. Bu suç bakımından görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun çerçevesinde (m. 8 ve 12) asliye ceza mahkemesidir.

Bilişim sistemlerine girme suçunda kovuşturmaya geçilirken basit yargılama usulünün uygulanmasına karar verilebilir.[52]

SONUÇ

Bilişim sistemlerine girme günümüz teknolojik gelişmeler karşısında çeşitli şekillerde gerçekleşmektedir. Bunlar bilişim alanında saldırı olarak kabul edilmektedir. Bilişim sistemlerine saldırılar çok çeşitli yöntemlerle yapılabilse de, sıklıkla karşılaşılanlardan biri oltalama (phishing) tekniğidir.[53] Saldırganlar, gerçek gibi görünen sahte e-postalar ve web siteleri kullanarak kullanıcıların kişisel bilgilerini veya kimlik bilgilerini çalmaya çalışır. Kötü amaçlı yazılımlar (malware), virüsler, truva atları, fidye yazılımları ve casus yazılımlar gibi kötü amaçlı yazılımlar, sistemlerin güvenliğini tehlikeye atarak verilere ve sistem işleyişine zarar verebilir. Dağıtılmış hizmet engellemede (DDoS saldırıları), saldırganlar çok sayıda bilgisayarı kullanarak hedeflenen sunucu, ağ veya web sitesine yoğun trafik gönderir ve hizmetleri geçici olarak durdurur veya yavaşlatır.[54] Bunlar dışında, SQL enjeksiyonu, kaba kuvvet (brute force) saldırıları, man-in-the-middle (MITM) saldırıları ve iç tehditler gibi çok çeşitli saldırı sınıfları bulunmaktadır.[55] Bu saldırılara karşı siber güvenlik önlemlerinin alınması ve sistemlerin düzenli olarak güncellenmesi, bu tür saldırılara karşı korunmak için önemlidir.

Bilişim sistemine girme genellikle başka suç tiplerinin işlenmesine aracılık eden bir fiildir. Bu fiillerin karşılığı 5237 sayılı TCK'da yer alsa bile sisteme girme fiilleri ile sistem içerisinde gerçekleşen fiilleri oluşturup oluşturmadığının açıklığa kavuşturulması gereklidir. Bu konuda çeşitli örnekler

52 YILMAZ, 206.

53 JOUNINI Mouna/RABAI Latifa Ben Arfa/AISSA Anis Ben, Classification of Security Threats in Information Systems, Procedia Computer Science, Cilt: 32, Yıl: 2014, (489-496), doi: 10.1016/j.procs.2014.05.452.

54 NIKOLSKAIA Kseniia/MINBALEEV Aleksey, Legal Regulation of Incidents Related to DDoS Attacks, *International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, Yaroslavl, Russia, Yıl: 2020, (53-55), doi: 10.1109/ITQMIS51053.2020.932.2874.

55 DHILLON Gurpreet/SMITH Kane(DISSANAYAKA Indika, Information Systems Security Research Agenda: Exploring the Gap Between Research and Practice, *The Journal of Strategic Information Systems*, Cilt: 30, Sayı: 4, doi: 10.1016/j.jsis.2021.101693.

verilebilir. Sık kullanılan akıllı şehir uygulamaları siber saldırılar ve veri ihlallerine karşı savunmasız olabilmektedir. Yaşanan son olaylardan biri 2018'de yaşanan Atlanta Ransomware Saldırısıdır.[56] ABD'deki Atlanta şehri, SamSam adlı bir fidye yazılımı saldırısına uğramış ve bu saldırı şehrin bilgi sistemlerine zarar vermekle kalmamış, yönetim hizmetlerinin kesintiye uğramasına sebep olmuştur. 2014 yılında ABD Michigan eyaletinde, bir grup araştırmacı trafiği kontrol etmek için kullanılan akıllı trafik ışığı sistemlerine sızarak sistemi manipüle etmiştir. Akıllı şehir uygulamaların hukuki boyutlarını inceleyen ulusal yayınlardan birinde otonom araçlar incelenmiştir.[57] Otonom araçlarda sürücü faktörü ortadan kalktığı için, meydana gelen trafik kazalarında; araç mekanik ve elektronik sistem üreticisi, yazılım geliştiricisi, altyapı hizmetlerinin sağlayacak olan yerel yönetimler ve araç malikinin hukuki ve cezai sorumlulukları konusunda birçok karışıklık oluşmaktadır.[58]

Saklanan kişisel verilerin korunması, sertifikasyon ve internet erişimlerinde standartların belirlenmesi, araçların sigortacılık sistemlerinin yeniden yapılandırılması, sorunların çözümünde evrensel yargılama yetkisine ihtiyaç duyulması birlikte değerlendirildiğinde tekelleşmeye, haksız rekabete veya ticari güç dayatmalarına sebep olabilmektedir. Akıllı şehirler için gereken yatırımlar ve atılacak adımlarda, hükümetler, yerel yönetimler, şehir plancıları, vatandaşlar ve şüphesiz hukukçuların bu ekosistem içinde oluşturulacak yönetişim mekanizmasına katılımı ve birbirleri ile iş birliği içinde olmaları şarttır.[59]

Bu açıklamalar hukukçulara bilişim teknolojilerinin basit bir uygulamanın ötesinde olduğunu, meydana gelecek olan fiillerin ciddi şekilde araştırılıp, suçta ve cezada kanunilik unsuru yönünden tespitini gerekli kılmaktadır. Bilişim sistemine girmenin ötesinde bu sistem içerisinde gerçekleşen fiillerin başka suçları oluşturması durumunda kanunlarımızın yetersiz kalmaması gerekliliği de çok önemlidir.

KAYNAKÇA

AKBULUT Berrin, Bilişim Alanında Suçlar, Adalet, Ankara, 2017.

APİŞ Özge, Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama, Elkoyma Koruma Tedbirleri, in: Yasama Dergisi, Cilt: 13, Sayı:37, Haziran 2018, (49-86).

BOADEN R./LOCKETT G., Information Technology, Information Systems and Information Management: Definition and Development, European Journal of Information Systems, Cilt 1, Sayı 1, Yıl:1991, (23-32).

CONGER Sue/PRATT Joanne/LOCH Karen, Personal Information Privacy and Emerging Technologies, Information Systems Journal, Haziran 2012, https://doi.org/10.1111/j.1365-2575.2012.00402.x, erişim tarihi: 4 Nisan 2023.

56 KRASZEWSKI Kenneth, SamSam and the Silent Battle of Atlanta, *in:* 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, Yıl: 2019, (1-16), doi: 10.23919/CYCON.2019.875.7090.

57 YETİM Servet, Sürücüsüz Araçlar ve Getirdiği / Getireceği Hukuki Sorunlar, *Ankara Barosu Dergisi*, Sayı:1, Yıl: 2016, https://dergipark.org.tr/tr/pub/abd/issue/33840/374707, erişim tarihi: 4 Nisan 2023.

58 TASTAN Yahya/KAYMAZ Habib, Otonom Araçların Önündeki Zorluklar, *International Journal of Advances in Engineering and Pure Sciences*, Cilt: 33, Sayı: 2, Yıl: 2021, (195-209), doi: 10.7240/jeps.741594.

59 DEMİRKIRAN Senem/YÜCEL Mehmet Ali/TERZİOĞLU M. Kenan/SELVİ Aslı, Dijital Dönüşüm Sürecinde Akıllı Yönetişim, *Journal of TESAM Academy*, Cilt: 8, Sayı: 2, (489-519), doi: 10.30626/tesamakademi. 971899.

DEMİRKIRAN Senem/YÜCEL Mehmet Ali/TERZİOĞLU M. Kenan/SELVİ Aslı, Dijital Dönüşüm Süre-cinde Akıllı Yönetişim, Journal of TESAM Academy, Cilt: 8, Sayı: 2, (489-519), doi: 10.30626/tesamakademi.971899.

DHILLON Gurpreet/SMITH Kane(DISSANAYAKA Indika, Information Systems Security Research Agenda: Exploring the Gap Between Research and Practice, The Journal of Strategic Information Systems, Cilt: 30, Sayı: 4, doi: 10.1016/j.jsis.2021.101693.

DÜLGER Murat Volkan, Bilişim Suçları ve İnternet, İletişim Hukuku, Seçkin, Ankara, 2015.

EGGERS William D./MACMILLAN, Paul, KAMU 2020: Kamunun Geleceğine Yolculuk, Deloitte, s. 6-8, 2015. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/tr-kamu%20 2020-kamunun %20gelecegine%20yolculuk.pdf, erişim tarihi: 6 Nisan 2023.

EKİCİ ŞAHİN Meral/ KORUCULU Irmak, Bilişim Sistemine Girme Suçu-Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarda İşlenmesine İlişkin Bir Değerlendirme, in: DEHFD, Prof.Dr. Durmuş Tezcan'a Armağan, Özel Sayı, Cilt I; İzmir 2019.

GÖÇOĞLU Volkan, Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine Bir İnceleme, MANAS Sosyal Araştırmalar Dergisi, Cilt 9, Sayı 1, Yıl: 2020, (615-628).

JOUNINI Mouna/RABAI Latifa Ben Arfa/AISSA Anis Ben, Classification of Security Threats in Information Systems, Procedia Computer Science, Cilt: 32, Yıl: 2014, (489-496), doi: 10.1016/j.procs.2014.05.452.

KARAKEHYA Hakan, Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu, Türkiye Barolar Birliği Dergi-si, Cilt: 22, Sayı: 81, Mart 2009, (187-210).

KOCA Mahmut, Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Ön-gördüğü Düzenlemeler ve Türk Hukuku, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, Cilt III, 2003.

KOCA Mahmut/ ÜZÜLMEZ İlhan, Türk Ceza Hukuku Özel Hükümler, Adalet, Ankara, 2022.

KRASZEWSKI Kenneth, SamSam and the Silent Battle of Atlanta, in: 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, Yıl: 2019, (1-16), doi: 10.23919/CYCON.2019.875.7090.

KÜZECİ Elif, Sayısal Fil, İnkılap, İstanbul, 2021.

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.1, YIL 2013.

NIKOLSKAIA Kseniia/MINBALEEV Aleksey, Legal Regulation of Incidents Related to DDoS Attacks, International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, Yıl: 2020, (53-55), doi: 10.1109/ITQMIS51053.2020.932.2874.

ÖNOK Murat, Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Ulus-lararası İşbirliği, in: Prof.Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırma-ları Dergisi, Cilt 19, Sayı 2, Yıl:2013, (ss.1229 – 1270).

SIEBER Ulrich, Bilişim Suçları, (çevirenler YENİSEY Feridun/ ZAİMOĞLU Damla); in: Bilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku, Seçkin, Ankara, 2021.

ÖZBEK Veli Özer/ DOĞAN Koray/ BACAKSIZ Pınar, Türk Ceza Hukuku Özel Hükümler, Seçkin, Ankara 2022.

TASTAN Yahya/KAYMAZ Habib, Otonom Araçların Önündeki Zorluklar, International Journal of Advances in Engineering and Pure Sciences, Cilt: 33, Sayı: 2, Yıl: 2021, (195-209), doi: 10.7240/jeps.741594.

TEZCAN Durmuş/ ERDEM Mustafa Ruhan/ ÖNOK Murat, Teorik ve Pratik Ceza Özel Hukuku, Seçkin, Ankara 2022.

WOOD-HARPER A.Trevor/ANTILL Lyn/AVISON David Ernest, Information Systems Definition: the Multi-view Approach, Blackwell Scientific Publications, United Kingdom 1985, (26-34).

YETİM Servet, Sürücüsüz Araçlar ve Getirdiği / Getireceği Hukuki Sorunlar, Ankara Barosu Dergisi, Sayı:1, Yıl: 2016, https://dergipark.org.tr/tr/pub/abd/issue/33840/374707, erişim tarihi: 4 Nisan 2023.

YILDIZ Ali Kemal, Bilişim Sistemine Girme, in: Özel Ceza Hukuku, Cilt VIII, Oniki Levha, İstanbul.

YILMAZ Sacit, Türk Ceza Hukuku Sisteminde Siber Suçlar, Adalet, Ankara 2023, 194.