Bilişim Suçlarında Hazırlık Hareketlerinin Cezalandırılması: TCK m.245/A Yasak Cihaz veya Programlar Suçu[*]

Punishment of Preparatory Acts in Cybercrimes: TPC art.245/A the Crime of Prohibited Devices or Programs

Veysel TOPUZ[**]

Öz:

24/03/2016 tarihli ve 6698 sayılı Kanun ile TCK'ya "yasak cihaz veya programlar" başlıklı 245/A maddesi eklenmiştir. Ülkemizin de taraf olduğu, Avrupa Konseyi Siber Suç Sözleşmesinin "cihazların kötüye kullanılması" başlıklı 6. maddesinde taraf devletlere, bilişim suçlarıyla ilgili hazırlık hareketlerinin ceza normuyla karşılanması hususunda bir yükümlülük yüklenmiştir. Ülkemiz de Sözleşmeye taraf olmanın bir gereği olarak ceza kanunumuzda bu fiilleri suç olarak ihdas etmiş, böylece Sözleşmede öngörülen yükümlülüğü yerine getirmiştir. Böylelikle bilişim suçlarıyla daha etkin mücadelenin sağlanması adına, cezalandırılabilirlik ön alana kaydırılmıştır. TCK m.245/A düzenlemesi önemli bir boşluğu doldurmuş vaziyettedir. Bu hüküm yalnızca bilişim suçlarının hazırlık hareketlerini değil bunun yanı sıra bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların da hazırlık hareketlerini cezalandırmaya elverişli olacak şekilde kaleme alınmıştır. Bununla birlikte hem suçun üst başlığı hem de hükmün formülasyonu önemli tartışmaları beraberinde getirmektedir. Bu tartışmalar özellikle kanunilik ilkesi bağlamında önem arz etmektedir. Ayrıca suçun oluşumu bakımından madde metninde sayılan nesneler bakımından bir sayı sınırının aranmıyor oluşu ve özellikle çift kullanım özelliği gösteren nesnelerin suça konu olup olamayacakları meselesi bu tartışmalarda önem arz etmektedir. Bu meselelerin Avrupa Konseyi Siber Suç Sözleşmesi ve açıklayıcı memorandumu bağlamında değerlendirilmesi gerekmektedir. Biz de çalışmamızda hem TCK m.245/A düzenlemesinde yer alan suçu, suç inceleme yöntemine uygun olarak inceleyeceğiz hem de yukarıda işaret ettiğimiz tartışmalı noktaları doktrindeki görüşler ve yargı kararları bağlamında değerlendirip görüşlerimizi ortaya koyacağız.

(*) Araştırma Makalesi / *Research Article*
Yayın Kuruluna Ulaştığı Tarih: 27.12.2024
Yayınlanmasının Kabul Edildiği Tarih: 25.02.2025
DOI: https://doi.org/10.58733/imhfd.1608701
Bu makaleye atıf için; TOPUZ, Veysel, "Bilişim Suçlarında Hazırlık Hareketlerinin Cezalandırılması: TCK m.245/A Yasak Cihaz veya Programlar Suçu", **İMHFD**, C. 10, S. 1, 2025, s. 237-273

(**) *Arş. Gör. Dr.*, İstanbul Medeniyet Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, İstanbul - Türkiye
E-posta: veyseltopuz_35@hotmail.com
Orcid: https://orcid.org/0000-0002-9831-2816

Anahtar Kelimeler:
Bilişim Suçları, Hazırlık Hareketleri, Yasak Cihaz ve Programlar, Avrupa Siber Suç Sözleşmesi.

Abstract:
Article 245/A titled "prohibited devices or programs" was added to the Turkish Penal Code by Law No. 6698 dated 24/03/2016. Article 6 of the Council of Europe Convention on Cybercrime, to which our country is a party, titled "misuse of devices" imposes an obligation on state parties to criminalize preparatory acts related to cybercrimes. As a requirement of being a party to the Convention, our country has criminalized these acts in our criminal code, thus fulfilling the obligation stipulated in the convention. Thus, in order to ensure a more effective fight against cybercrimes, punishability has been shifted to the front area. Article 245/A of the TPC has filled an important gap. This provision has been drafted to punish not only the preparatory acts of cybercrimes, but also the preparatory acts of other crimes that can be committed by using information systems as a tool. Nevertheless, both the title of the offense and the formulation of the provision bring important discussions. These discussions are especially important in the context of the principle of legality. In addition, the fact that a number limit is not sought for the objects listed in the text of the article in terms of the formation of the offense and especially the issue of whether objects with dual use characteristics can be subject to the crime is important. These discussions should be evaluated in the context of the Council of Europe Convention on Cybercrime and its explanatory memorandum. In our study, we will examine the offense under Article 245/A of the TPC in accordance with the crime investigation method, and we will evaluate the controversial points mentioned above in the context of the opinions in the doctrine and judicial decisions and put forward our opinions.

Keywords:
Cybercrimes, Preparatory Acts, Prohibited Devices and Programs, European Convention on Cybercrime.

GİRİŞ

Bilgisayarlar ve diğer elektronik cihazların yanı sıra internetin yaygınlaşması, günlük yaşamda birçok kolaylık sağlamaktadır. Bilişim sistemlerinin her geçen gün gelişmesi artık birçok işlemin bilgisayar veya mobil cihazlar üzerinden çok hızlı şekilde yapılmasına imkan sağlar hale gelmiştir. Ancak bu kolaylık bazı olumsuzlukları da beraberinde getirmektedir. Özellikle ceza hukuku açısından değerlendirdiğimizde geleneksel birçok suçun yeni işleniş şekilleri ile karşılaşılmaktadır ve suçların takibi oldukça zor hale gelmektedir.

Bilişim teknolojilerindeki ilerlemeler, bilişim sistemlerini günlük yaşamımızın vazgeçilmez bir parçası haline getirmiştir. Özellikle bilişim suçlarının sınır aşan yapısı ve her geçen gün fiillerin işleniş şeklinin de farklılık arz etmesi dolayısıyla bu suçlarla mücadele bakımından yeni düzenlemelerin yapılması ve var olan suç türlerine yeni türlerin eklenmesi zorunlu hale gelmiştir[1]. Üstelik

[1] KAYA, İslam Safa/ÇAKIR, Adem, "Yasak Cihaz veya Programlar Suçu", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, Y. 2020, C. 19, Sa: 38, s. 33; TAŞKIN, Şaban Cankat, Ceza Hukukunda Ceza-

uluslararası sözleşmelerle taraf devletlere bu hususta yükümlülükler de yüklenmektedir.

Sözlük anlamı olarak bilişim "*teknik, ekonomik ve toplumsal alanlardaki iletişimde kullanılan ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi*" olarak tanımlanabilir[2]. Bilişim, insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, yeniden üretilmesi, bilginin bilgisayarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimi olarak tanımlanabilir[3].

Bilişim kavramına ceza mevzuatımızda ilk kez 1989 tarihli Türk Ceza Kanunu Ön Tasarısında rastlanmaktadır. Ön tasarının 342. maddesinin gerekçesinde, bilişim alanı, *"bilgileri toplayıp depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinden oluşan alan"* olarak tanımlanmıştır. 1997 ve 2000 tarihli TCK tasarılarının gerekçesinde de *"verileri toplayıp, yerleştirdikten sonra bunları otomatik işleme tabi tutma imkanı veren manyetik sistemler"* olarak tanımlanmıştır[4].

Siber suçların sınır aşan yapısı dolayısıyla bunlarla mücadele etme bakımından en başta gelen hususlardan birisi uluslararası adli yardımlaşmadır[5]. Devletler ve uluslararası örgütler siber suçlarla bütüncül bir mücadeleyi mümkün

landırılabilirliğin Ön Alana Kaydırılması ve Hazırlık Hareketlerinin Cezalandırılması Sorununun Yasak Cihaz veya Programlar Suçu Özelinde İngiliz Ceza Hukuku, Kanada Ceza Hukuku ve Avrupa Konseyi Siber Suç Sözleşmesindeki Düzenlemelerle, **Ceza Hukuku Dergisi**, Ağustos 2024, C. 19 Sa. 55, s. 252; KARADENİZ, Yusuf, "Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ve Türk Hukuku'nda Karşılığı", **Güvenlik Bilimleri Dergisi,** Y. 2022, C. 11, Sa: 1, s. 111-114; EREN, Ahu Karakurt, "Bilişim Alanında Suçların veya Bilişim Sistemlerinin Araç Olarak Kullanıldığı Diğer Suçların İşlenmesi Amacıyla Cihaz, Program, Şifre ya da Güvenlik Kodlarının Üretilmesi, Yayılması veya Bulundurulması Suçu", **Türkiye Adalet Akademisi Dergisi,** Y. 2020, Sa: 43, s. 221-222; TUNÇER, Asuman İnce, "Yasak Cihaz ve Programlar Suçu (TCK m.245/A)", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Y. 2024, C. 32, Sa: 3, s. 1298; ALİUSTA Cahit/Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, 2018, C. 4, Sa: 2, s. 35.

2 https://sozluk.gov.tr/, E.T. 20/12/2024.

3 DÜLGER, Murat Volkan, **Bilişim Suçları ve Internet İletişim Hukuku**, Genişletilmiş ve Güncellenmiş 8. Baskı, Seçkin Yay., İstanbul, 2020, s. 66; YENİDÜNYA, A. Caner/DEĞİRMENCİ, Olgun, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, Legal Yayıncılık, İstanbul, 2003, s. 27; KARAGÜLMEZ, Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Genişletilmiş ve Gözden Geçirilmiş 3. Baskı, Seçkin Yay., Ankara, 2011, s. 41; MERAN, Necati, **Sahtecilik - Malvarlığı Bilişim Suçları ile Ekonomik ve Ticaret Alanında Suçlar**, Genişletilmiş ve Gözden geçirilmiş 2. Baskı, Seçkin Yay., Ankara, 2008, s. 564; ERMEYDAN, Damla, **Türk Ceza Kanununda Bilişim Suçları**, Güncellenmiş 2. Baskı, Seçkin Yay., Ankara, 2023, s. 28.

4 DÜLGER, s. 69; YENİDÜNYA/DEĞİRMENCİ, s. 43; KARAGÜLMEZ, s. 133; MERAN, s. 564; AKBULUT, Berrin, **Bilişim Alanında Suçlar**, 2. Baskı, Ankara, Adalet Yayınevi, 2017, s. 13.

5 ÖNOK, Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 19, No: 2, 2013, (ss. 1229-1270), s. 1232; KARADENİZ, s. 114; EREN, s. 222; ALİUSTA/ BENZER, s. 40.

hale getirmek amacıyla önemli girişimlerde bulunmuşlardır[6]. Bu bağlamda imzalanan en önemli anlaşmalardan bir tanesi 2001 tarihli Siber Suç Budapeşte Sözleşmesidir. Devletlerin imzasına 23 Kasım 2001'de Budapeşte'de açılan Siber Suç Sözleşmesi, 1 Temmuz 2004'te yürürlüğe girmiş olup bu alandaki ilk uluslararası sözleşme olma özelliği göstermektedir[7].

Bilişim alanındaki suçların cezalandırılabilirliğinin hazırlık hareketlerine doğru ilerlemesinin en önemli sebeplerinden bir tanesi devletler arasındaki işbirliği arzusudur[8]. "Avrupa Suç Sorunları Komitesinin CDPC/103/211196 sayılı kararıyla" bilişim suçlarıyla ilgili belirli alanları inceleyerek bağlayıcı bir hukuki metin ortaya koymak amacıyla bir uzmanlar komitesi oluşturulmuştur[9]. Bu komitenin çalışmaları sonucunda Avrupa Konseyi Siber Suç Sözleşmesi ve sözleşmenin açıklayıcı raporu (memorandum) hazırlanmıştır. Sözleşme, uluslararası düzlemde bilişim alanında yapılmış en kapsamlı düzenleme olma niteliğini haizdir[10].

Türkiye Sözleşmeye 10/11/2010 tarihinde imza koymuş, 22/04/2014 tarih ve 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesi[11] adıyla onaylanması uygun bulunmuş ve Sözleşme 02/05/2014 tarihinde yürürlüğe girmiştir[12]. Sözleşmenin "*cihazların kötüye kullanılması*" başlıklı 6. maddesiyle "bilişim suçlarıyla ilgili hazırlık hareketlerinin cezalandırılması" öngörülmüştür. Buna göre taraf devletler; "yasadışı erişim (madde 2), yasadışı araya girme (madde 3), verilere müdahale (madde 4), sisteme müdahale (madde 5) suçlarını işlemek gayesiyle bilgisayar programı, cihaz, şifre, erişim kodu veya benzer bir veri oluşturmayı ve imal etmeyi" suç haline getirmekle yükümlü kılınmışlardır.

---

6 ÜNAL, Osman Gazi, "Cezalandırılabilirliğin Ön Alana Kaydırılması Bağlamında, Yasak Cihaz veya Programlar Suçu (TCK m.245/A)", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C. 26, Sa: 2, 2022, s. 591; ÖNOK, s. 1232; ALİUSTA/BENZER, s. 36.

7 İÇEL, Kayıhan, Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri, **İstanbul Hukuk Mecmuası,** C. 59, Sa: 1-2, Y. 2011, s. 6; ÖNOK, s. 1232-1233; KARADENİZ, s. 114-115; ERMEYDAN, s. 97; ALİUSTA/BENZER, s. 38.

8 PUSCHKE, Jens, "**Grund und Grenzen des Gefährdungsstrafrechts am Beispiel der Vorbereitungsdelikte", Roland Hefendehl** (Ed.), Grenzenlose Vorverlagerung des Strafrechts?, Berliner Wissenschafts Verlag, 2010, s. 17. (akt. ÜNAL, s. 596; İÇEL, s. 5).

9 ÜNAL, s. 596-597.

10 SIEBER, Ulrich vd., B**ilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku,** Birinci Baskı: Mayıs 2021, Ankara, Seçkin, 2021, s. 268.

11 https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenenSuclar.pdf, E.T. 22/12/2024.

12 22/4/2014 tarihli ve 6533 sayılı Kanunla uygun bulunmuştur.

Sözleşmenin bu maddesi, bilişim suçlarıyla daha etkin mücadele edilmesini sağlamak adına cezalandırılabilirliği bir nevi hazırlık hareketlerine kaydırmakta, taraf devletlere bu alanda düzenleme yapılması hususunda yükümlülük yüklemektedir[13].

Bizim mevzuatımız bakımından da konu tartışılmış ve doktrinde bilişim suçlarının işlenmesine yönelik hazırlık hareketlerinin cezalandırılmasını sağlayacak bir hükmün bulunmayışı eleştiri konusu olmuştu[14]. Nitekim kanun koyucu, bu eksikliği gidermek maksadıyla 24/03/2016 tarihli ve 6698 sayılı Kanun ile birlikte TCK'ya 245/A maddesi olarak aşağıda yer verilen hükmü eklemiştir:

> *"Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır".*

Bizim Kanunumuza hâkim olan temel prensiplerden bir tanesi de kural olarak hazırlık hareketlerinin cezalandırılmaması ilkesidir[15]. Hazırlık hareketleri cezalandırılabilir hareketler değildir[16]. Bununla birlikte bazı hallerde hazırlık

---

13 ÜNAL, s. 598; EREN, s. 222; KOCA, Mahmut/ÜZÜLMEZ, İlhan, **Türk Ceza Hukuku Özel Hükümler**, 10. Baskı, Adalet Yayınevi, Eylül 2024, s. 1070-1071.

14 DÜLGER, s. 484. KOCA/ÜZÜLMEZ, **Ceza Özel**, s. 1071.

15 ÖZGENÇ, İzzet, **Türk Ceza Hukuku Genel Hükümler**, 20. Baskı, Seçkin Yayıncılık, Ankara 2024, s. 568; KOCA/ÜZÜLMEZ, Ceza Genel, s. 422; ÖZBEK, Veli Özer/ DOĞAN Koray/MERAKLI, Serkan/ BACAKSIZ, Pınar/Başbüyük, İsa, **Türk Ceza Hukuku Genel Hükümler**, 15. Baskı, Seçkin Yayıncılık, 2024, s. 483; ARTUK, Mehmet Emin/GÖKCEN, Ahmet/ALŞAHİN, M. Emin/ÇAKIR, Kerim, **Ceza Hukuku Genel Hükümler**, 18. Baskı, 2024, s. 673; İÇER, Zafer, **Suça Teşebbüste Hazırlık Hareketleri ile İcra Hareketlerinin Birbirinden Ayrılması**, On İki Levha Yayıncılık, Haziran 2021, s. 37. Hazırlık hareketlerinin cezalandırılmasıyla ilgili Türk doktrininde son zamanlarda önemli çalışmalar ortaya konulmuştur. Hazırlık hareketlerinin cezalandırılabilirliğine ilişkin görüşler için TAŞKIN, s. 257; YETKİN, Erdi, **Cezalandırılabilirliğin Öne Alınmasının Bir Görünüş Biçimi Olarak Hazırlık Hareketlerinden Doğan Ceza Sorumluluğu**, İstanbul Arşivi, On İki Levha Yayıncılık, Şubat 2024, s. 306. Devletin cezalandırma yetkisini sınırlandırmak için hazırlık hareketlerinin cezasızlığına ilişkin bkz. YETKİN, s. 384. ÖZGÜÇ, Levent Emre, **Türk Ceza Hukukunda Hazırlık Hareketlerinin Belirlenmesi ve Cezalandırılabilirliği**, On İki Levha Yayıncılık, Ağustos 2024, s. 127, 128; KERMAN, Onur Kemal, Hazırlık Hareketlerinin Cezalandırılması, **Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yayımlanmamış Doktora Tezi**, Mart 2024, s. 127. Ayrıca bkz. ÖZGÜÇ, Levent Emre, 5846 Sayılı Fikir ve Sanat Eserleri Kanunu m.72'de Yer Alan "Teknolojik Önlemleri Etkisiz Kılma" Suçunun Değerlendirilmesi, Suç Genel Teorisi ve Ceza Adaleti Bağlamında Güncel Mevzuat Değişikliklerine İlişkin Değerlendirmeler, **İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Ceza Hukuku Sempozyumu Tam Metin Bildirileri Kitabı**, Nisan 2024, s. 139.

16 ÖZGENÇ, s. 563; KERMAN, s. 95.

hareketleri bizatihi cezalandırılabilir nitelikte hareketler olarak müstakil bir suç tipini oluşturulabilir[17]. TCK m.245/A da bunlardan bir tanesidir[18].

Genel kural olarak hazırlık hareketlerinin cezalandırılmaması ve bazı istisnai durumlarda cezalandırılması, doktrinde çeşitli gerekçelerle açıklanmaya çalışılmış bir konudur[19]. Aslında, hem cezasızlığa hem de istisnai cezalandırmaya yönelik gerekçeler, birbirini tamamlayan iki farklı bakış açısı olarak değerlendirilebilir. Hazırlık aşamasında, eylemlerin sürdürülüp sürdürülmeyeceği veya nasıl devam edeceği belirsizdir[20]. Hazırlık hareketlerinin cezalandırılması, genel olarak bu tür eylemlerin neden cezalandırılmadığını açıklayan argümanların bir istisnası olarak görülebileceği gibi, bu gerekçelerden bir sapma veya bunlardan vazgeçiş olarak da değerlendirilebilir[21].

Hazırlık hareketlerinin cezasız bırakılması, failin suç işleme niyetinden vazgeçmesi için güçlü bir teşvik unsuru oluşturur. Ayrıca, hazırlık hareketlerinde failin amacını kesin olarak kanıtlamak önemli bir zorluk teşkil eder[22]. Kanaatimce bir hazırlık hareketinin cezalandırılmasının meşruiyet taşıyabilmesi için hedef suçun ağır bir nitelikte olması ve önemli bir hukuki değeri koruması gerekir[23]. Bu bağlamda öncelikle kural olarak hedef suçun bir zarar suçu olması gerekir, eğer bir tehlike suçu ise hazırlık normunun düzenlenmesinde daha da fazla titiz davranılmalıdır[24]. Bu kapsamda hazırlığın istisnai olarak cezalandırılması kuralına uyulmalı, genel hazırlık sorumluluğundan kaçınılmalıdır. Cezalandırılabilirliğin öne alınmasında anayasal koşullara, çekirdek alan korumasına, belirlilik ilkesine, kusur ilkesine ve ölçülülük ilkesine riayet edilmelidir[25].

---

17 "Örneğin, TCK m.220'de yer alan suç işlemek amacıyla örgüt kurma, TCK m.200'de yer alan parada ve kıymetli damgaları yapmayı yarayan araçlar suçu, TCK m.227/1'de yer alan ve fuhuş suçunun işlenişine yönelik hazırlık hareketlerinin de tamamlanmış suç gibi cezalandırılmasını öngören hükümler". ÜNAL, s. 599. Hazırlık hareketleri de cezalandırılabilir ancak temel koşul olarak cezalandırılan hazırlık hareketinin haksız olması gerekir şeklindeki görüş için bkz. YETKİN, s. 388. Benzer görüş için bkz. ÖZGÜÇ, Hazırlık.., s. 167, 175. Hazırlık hareketlerinin cezalandırılmasında kendi suçuna hazırlık, başkasının suçuna hazırlık, karma hazırlık şeklindeki ayrımlar için bkz. YETKİN, s. 267, 269; ÖZGÜÇ, Hazırlık.., s. 148. Klasik hazırlık hareketleri örnekleri için bkz. İÇER, s. 38-41, KERMAN, s. 112.

18 TCK m.245/A'nın kimi zamanlarda kendi suçuna hazırlık kimi zamanlarda ise bir başkasının suçuna hazırlık özelliği gösterdiğine ilişkin görüş için bkz. ÖZGÜÇ, Hazırlık..., s. 149.

19 YETKİN, s. 306.

20 YETKİN, s. 306 vd.

21 YETKİN, s. 306 vd. Hazırlık hareketlerinin cezalandırılmasına dair görüşlerin temelinde ise iki husus öne çıkar. Bunlardan ilki korunan hukuki değerin özellikli önemi-ilgili hazırlık hareketinin tehlikeliliği ve erkenden müdahale yetkisi oluşturma amacıdır. YETKİN, s. 317 vd. Yazarın kendi görüşü için ise bkz. YETKİN, s. 349 vd.

22 YETKİN, s. 306.

23 YETKİN, s. 388 vd.

24 YETKİN, s. 388 vd.

25 YETKİN, s. 388 vd.

Hazırlık hareketlerini cezalandıran TCK m.245/A düzenlemesiyle ilgili olarak da doktrinde hükmün gerekliliğine ve içeriğine dair önemli tartışmalar mevcuttur. Öncelikli suçun düzenlendiği madde başlığının "yasak cihaz veya programlar" olarak belirlenmesinin doğru bir tercih olmadığı belirtilmektedir[26]. Madde başlıklarının seçiminde fiil unsurunun ön plana çıktığı, oysa TCK m.245/A bakımından suçun konusu olan unsurlara madde başlığında yer verildiği bundan dolayı madde başlığının madde içeriği ile uyuşmadığı, içeriği yansıtmadığı ileri sürülmektedir[27]. Biz de bu eleştirilere katılmaktayız. Bir kere madde başlığında 'yasak' ibaresi geçmekle birlikte madde metninde bu ibare geçmemektedir. İkincisi madde başlığında fiil unsuruna yer verilmemesi içerik ile başlığın uyumsuzluğu sorununu beraberinde getirmektedir. Tüm bu nedenlerle madde başlığının "cihaz veya programların kötüye kullanılması" şeklinde değiştirilmesi yönünde bir tercihte bulunulabileceği kanaatindeyiz[28]. Üstelik bir üst madde olan 245. maddenin de başlığının "banka veya kredi kartlarının kötüye kullanılması" olması düşüncemizi destekler mahiyettedir.

Hükmün gerekçesinde, Avrupa Siber Suçlar Sözleşmesi'nin (ASSM) 6. maddesine atıfta bulunulmakta ve taraf devlet olmanın gereği olarak belirlenen yükümlülüğün yerine getirildiği ifade edilmektedir. Bu maddede, bilişim suçlarının ve bilişim sistemlerinin suç işlemek amacıyla araç olarak kullanıldığı eylemlerle ilgili olarak, caydırıcı ve etkin bir mücadele sağlamak amacıyla bu tür fiillerin cezai yaptırımlarla karşılanmasının önemli olduğu vurgulanmaktadır[29].

Bu suç tipinin ihdasıyla bilişim alanındaki suçlarda cezalandırılabilirliğin hazırlık hareketlerine doğru kaydırılması hem ASSM sözleşmesinde öngörülen yükümlülüğün yerine getirilmesi hem de bu suçlarla daha etkin mücadelenin sağlanması adına isabetli olmuştur[30]. Bilişim alanında yaşanan baş döndürücü gelişmelerin de etkisiyle hem yeni yeni tehditler ortaya çıkmış hem de suçların

---

26 AKBULUT, s. 348; ÖZBEK, Veli Özer/KORAY Doğan/PINAR Bacaksız, **Türk Ceza Hukuku Özel Hükümler**, Genişletilmiş ve güncellenmiş 18. baskı, Seçkin Yayıncılık, Eylül 2023, Ankara, 2023, s. 1056.

27 AKBULUT, s. 348; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler,** s. 1056.

28 AKBULUT, s. 348. Yazar aynı yerde, tıpkı TCK m.245'te olduğu gibi "program veya cihazların kötüye kullanılması" başlığının tercih edilebileceğini belirtmektedir. Özbek vd.'ne göre ise madde başlığı suçta kullanılacak cihaz ve programların üretilmesi, yayılması veya bulundurulması" şeklinde tercih edilebilir. ÖZBEK/DOĞAN/BACAKSIZ, **Ceza Özel**, s. 1057.

29 TAŞKIN, s. 263; ÜNAL, s. 600; TEKİN, Derya, "Bir Ceza Politikası Olarak Hazırlık Hareketlerinin Cezalandırılması: Türk ve İngiliz Yasal Düzenlemelerinin Karşılaştırmalı Analizi", **Terazi Hukuk Dergisi**, C. 13, No: 147, 2018, (ss. 48-60), s. 52.

30 TEKİN, s. 52. Yazar aynı yerde söz konusu TCK m.245/A düzenlemesinin Uluslararası Ceza Hukuku Derneği'nin standartlarına (AIDP) da tam bir uygunluk içerisinde olduğunu belirtmektedir.

işleniş şekilleri her geçen gün değişmiştir. Getirilen bu hüküm bu nedenle önemli bir boşluğu doldurmuş durumdadır[31].

I. MUKAYESELİ HUKUKTAKİ DÜZENLEMELER

Çeşitli ülkelerin düzenlemelerine bakıldığında bilişim alanında gerçekleştirilen fiillerin cezalandırılmasında temelde iki sistemin söz konusu olduğu görülmektedir[32]. Örneğin Amerika Birleşik Devletleri, İngiltere gibi bazı ülkeler, bilişim suçlarıyla ilgili özel, münhasır bir kanun yapma yolunu tercih ederlerken, Almanya, İsviçre, İtalya, Hollanda gibi diğer ülkeler ise temel ceza kanunlarının içinde bu suçları düzenleme yoluna gitmektedirler[33]. Türkiye, bilişim suçlarını düzenleme bakımından ikinci sistemi tercih eden bir ülkedir.

Avrupa Konseyi Siber Suç sözleşmesinin 6. maddesinde getirilen, bilişim suçlarının hazırlık hareketlerinin cezalandırılmasına ilişkin yükümlülüğün birçok taraf devlet tarafından yerine getirildiğini görmekteyiz. Çalışmamızın devamında mukayeseli hukukta bazı ülkelerdeki bu alanda yapılan benzer düzenlemeleri inceleyeceğiz.

A. Amerika Birleşik Devletleri

Hem bilgisayarın bulunması ve buna ilişkin dünyadaki en önemli teknolojik gelişmelerin yapıldığı ülke olması hem de internetin ilk olarak geliştirildiği ve yaygınlaştığı yer olması dolayısıyla ABD, bilişim suçlarının ilk ortaya çıktığı ve haliyle bu suçların düzenlenmesine ilk ihtiyaç duyulan yerdir[34].

ABD'nin önemli bir özelliği, Avrupa Konseyi üyesi olmamasına rağmen "Avrupa Siber Suç Sözleşmesini" imzalamış ve taraf olmuş olmasıdır[35]. Bundan dolayı Avrupa Siber Suç Sözleşmesinde yer alan yetki ve yükümlülükler ABD açısından söz konusudur[36].

Bilişim alanındaki bazı ihlalleri suç tipi haline getiren Amerikan Temel Yasasının (*US Code*[37]) 18. bölümünün (*Crimes and Criminal Procedure*) 1029.

---

31 ÖZBEK/DOĞAN/BACAKSIZ, **Ceza Özel**, s. 1056.

32 AKBULUT, s. 90.

33 AKBULUT, s. 91; DÜLGER, s. 213.

34 DURSUN, Selman, "İnternetten Kaynaklanan Ceza Sorumluluğundaki Gelişmeler", MHB, C. 3, **Prof. Dr. Ünal Tekinalp'e Armağan**, Sa: 1-2, 2003, s. 254; ÇEKEN, Hüseyin, "Amerika Birleşik Devletlerinde İnternet Yolu ile İşlenen Suçlara İlişkin Düzenlemeler", **Askeri Adalet Dergisi**, Sa. 144, 2002, s. 73; ERDOĞAN, s. 54.

35 DÜLGER, s. 214.

36 DÜLGER, s. 214.

37 US Code ifadesini bundan sonra USC diye kısaltacağız.

maddesinin (*Fraud and related activity in connection with access devices*) değiştirilmesi yoluyla yapılan 1984 tarihli Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Yasası (*Computer Fraud and Abuse Act 1984, CFAA*) bu alandaki en önemli ve temel düzenlemedir[38]. 18 USC §1029 erişim cihazlarıyla bağlantılı dolandırıcılık ve ilgili faaliyetler başlığını taşımaktadır. Bu hüküm bizim ceza kanunumuzdaki banka veya kredi kartlarının kötüye kullanılması başlığını taşıyan TCK m.245 hükmüne benzemektedir. Amerikan kanun koyucusu banka veya kredi kartı terimini kullanmak yerine erişim cihazı terimini kullanmıştır.

Erişim cihazı terimi aynı hükmün sonunda yer alan tanımlar maddesinde "*tek başına veya başka bir erişim aygıtıyla birlikte para, mal, hizmet veya başka bir değerli şey elde etmek için kullanılabilen veya bir fon transferini başlatmak için kullanılabilen (sadece kağıt belgeyle başlatılan bir transfer hariç) herhangi bir kart, plaka, kod, hesap numarası, elektronik seri numarası, mobil kimlik numarası, kişisel kimlik numarası veya diğer telekomünikasyon hizmeti, ekipmanı veya araç tanımlayıcısı veya diğer hesap erişim araçları anlamına gelir*" şeklinde tanımlanmıştır. Görüldüğü üzere erişim cihazı terimi, banka veya kredi kartı terimlerine göre daha geniş bir içeriğe sahiptir. Bu bağlamda örneğin mobil bankacılık uygulamasına girerken kullanılan parola/şifre gibi kodlar da erişim cihazı sayılacaktır.

Bu hükmün a (§ 1029/a) fıkrasının 4 numaralı alt bendinde bizdeki TCK 245/A düzenlemesine benzer bir düzenleme söz konusudur[39]. Buna göre, sahte erişim cihazı üretmek için cihaz yapım ekipmanı bulundurmak, üretmek, ticaretini yapmak, muhafaza etmek yasaklanmıştır. Hükmün tanımlar maddesinde cihaz yapım ekipmanı terimi, "*bir erişim cihazı veya sahte bir erişim cihazı yapmak için tasarlanmış veya öncelikli olarak kullanılan herhangi bir ekipman, mekanizma veya baskı anlamına gelir*" şeklinde tanımlanmıştır.

Bu suçun işlenmesine teşebbüs eden kişiler de tamamlanmış suçu işlemiş gibi cezalandırılacaktır[40]. Suçun cezası ise 1029. maddenin C bölümünde 15 yılı aşmayan hapis cezası ya da adli para cezası ya da her ikisinin birlikte verilmesi gerektiğine ilişkindir. Amerikan sisteminde işlenmiş bir suçtan daha önce bulunan

---

38 USC tam metni için bkz. https://uscode.house.gov/, E.T. 22/12/2024.

39 18 USC §1029/a/4.

40 Amerikan hukukunda bu durum "inchoate offense" olarak isimlendirilir. Başlangıç aşamasındaki suç olarak tercüme edilebilen bu kavram başka bir suçun işlenmesine yönelik cezalandırılabilir bir fiil içeren suçlar olarak tanımlanabilir. https://www.law.cornell.edu/wex/inchoate_offense, E.T. 05/02/2025.

mâhkumiyet yani bizdeki tekerrür kurumu doğrudan cezayı artırmayı gerektiren bir durum olarak düzenlenmiştir. Dolayısıyla önceden işlenmiş başka bir suçtan mâhkumiyeti varsa suçun cezası 20 yıla kadar hapis cezasına çıkmaktadır.

B. Kanada

Kanada Ceza Kanunu'nun 9. bölümü "mülkiyet hakkına karşı suçlar" başlığını taşımaktadır. Bu bölümde kredi kartlarıyla ilgili sahtecilik, hırsızlık gibi fiiller müeyyide altına alınmaktadır[41]. Kanunun "hırsızlığa benzeyen suçlar" (*Offences Resembling Theft*) başlıklı bölümünün 342. maddesinde kredi kartlarına yönelik hukuka aykırı fiiller müeyyide altına alınmaktadır.

Kanada Ceza Kanunu da bizdeki TCK m.245/A düzenlemesine benzer düzenlemeler içermektedir. Kanada kanun koyucusu bizden farklı olarak bilişimle ilgili her bir suçun altına bizdeki TCK m.245/A'ya benzer bir düzenleme getirmiştir. Bir diğer ifadeyle bizim Kanunumuzda TCK m.245/A bilişim sistemi ve bilişim sisteminin araç olarak kullanıldığı tüm suçları kapsamakta iken, Kanada Kanun koyucusu kredi kartlarında sahtecilik suçunun altında ayrı, bilişim sistemine yetkisiz girme suçunun altında ayrı olacak şekilde daha kazuistik bir düzenleme getirerek bu suçların işlenmesini sağlayacak cihaz, aparat, malzeme bilgisayar programının yapılmasını, üretilmesini, ihraç edilmesini vs. yasaklamıştır. Kısaca bunlara bakacak olursak:

Örneğin, Kanada CK'nun mülkiyete karşı suçlar başlıklı 9. bölümünün 342.01 no.lu maddesinde kredi kartı verilerini kopyalamaya, sahte kredi kartı üretmeye veya taklidini yapmaya yönelik herhangi bir alet, cihaz, aparat, malzeme veya diğer bir şeyi yapan, onaran, satın alan, satan, Kanada'dan ihraç eden, Kanada'ya ithal eden veya bulunduran bir kişinin suç işlemiş sayılacağı ve 10 yılı aşmayan bir hapis cezasına çarptırılabileceği düzenlenmiştir. Bu cihazların müsadere edileceği hüküm altına alınmıştır[42].

Benzer bir düzenleme Kanada CK'nın 342.2 no.lu maddesinde de söz konusudur[43]. Bu madde de bilişim sistemine yetkisiz girme eyleminin işlenmesini sağlamak amacıyla tasarlanmış veya uyarlanmış bir cihazın yapılmasını, bulundurulmasını, satılmasını, satışa sunulmasını, ithal edilmesini, kullanılmasını, dağıtılmasını veya kullanıma sunulmasını yasaklamaktadır.

---

41 Kanada Ceza Kanunu için bkz. https://laws-lois.justice.gc.ca/eng/acts/C-46/page-50.html#h-121811, E.T. 22/12/2024.

42 https://laws-lois.justice.gc.ca/eng/acts/c-46/page-51.html#docCont, E.T. 22/12/2024.

43 https://laws-lois.justice.gc.ca/eng/acts/c-46/page-51.html#docCont, E.T. 22/12/2024.

II. KORUNAN HUKUKİ DEĞER

Bu suç tipiyle, bilişim suçlarının ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilecek suçların hazırlık hareketlerine bir cezai müeyyide öngörülerek cihaz, bilgisayar programı, şifre ve sair güvenlik kodunun imal edilmesi, depolanması ve dolaşıma sokulması yasaklanmaktadır[44].

Bu suç tipi bakımından korunan hukuki değer, esasen diğer bilişim suçlarıyla korunan ile benzerdir. Bireylerin, bilişim sistemlerinin doğru ve hatasız işleyişine ilişkin güvenleri korunmaktadır. Bilişim sistemleri aracılığıyla insanlar, bankacılık işlemleri, iletişim, ticari ilişkiler gibi birçok alanda hizmet almakta ve haliyle bu alanlar ceza hukukuyla korunmaya muhtaç hale gelmektedir. Bu suç tipi aynı zamanda bir tehlike suçu olduğundan toplum güvenliği de korunmaktadır[45].

Bu suç tipiyle korunan hukuki değerin yalnız başına bilişim sistemlerinin güvenilir işleyişine ilişkin toplumda oluşan güvenin olduğunu söylemek ise yeterli bir yaklaşım olmayacaktır. Zira bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar da bu suçun ilgi alanına girdiğinden diğer suçlarla korunan hukuki değerler de bu suç tipiyle korunmaktadır[46,47]. Bu bağlamda bu suçla korunan hukuki değerin karma bir nitelik arz ettiği söylenmelidir[48]. Örneğin, bir başkasının özel hayatına ilişkin görüntü veya seslerini sosyal medya platformlarında ifşa etmek amacıyla bir bilgisayar programının yapılması halinde hem özel hayatın gizliliği hem de bilişim sisteminin güvenilir işleyişi korunması gereken hukuki değerleri oluşturur[49]. Ya da başkasına ait gerçek bir kredi kartının kopyalanmasını sağlayan bir cihazın yasaklanmasıyla aynı zamanda kişilerin malvarlığı değerlerinin de korunmuş olacağı izahtan varestedir.

---

44 KOCA/ÜZÜLMEZ, **Özel Hükümler**, s. 913.

45 ÜNAL, s. 606; KAYA/ÇAKIR, s. 42; GÜL, Ahmet, **Doğrudan-Dolaylı Bilişim Suçları**, Genişletilmiş, güncellenmiş ve yenilenmiş 3. baskı, Ankara, Seçkin Yayıncılık, 2021, s. 347; AKBULUT, Bilişim Alanında Suçlar, s. 349.

46 TUNÇER, s. 1303. Hazırlık suçlarının, tehlike suçu olup olmayacağına ilişkin tartışmalar ve TCK m.245/A ve Alman Ceza Kanunu 202c maddesi bağlamında değerlendirmeler için bkz. KEÇELİOĞLU Elvan Keçelioğlu, "Sırf Hareket Suçu Soyut Tehlike Suçu Mudur?", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi** C. 25, Sa. 2, 08 Mayıs 2021, s. 458-459. Hazırlık suçu tehlike suçu arasındaki ilişki için bkz. YETKİN, s. 237 vd.

47 DÜLGER, s. 488.

48 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1057.

49 KAYA/ÇAKIR, s. 44.

III. SUÇUN UNSURLARI

A. Tipikliğin Maddi Unsurları

1. Fail

Suçun faili olmak bakımından Kanunda herhangi bir özellik aranmamıştır. Haliyle herkes bu suçun faili olabilir[50]. Maddede sayılan fiilleri gerçekleştirmek için failin bilgisayar veya bilişim uzmanı, hacker veya korsan olmasına gerek yoktur. Yasak cihaz veya programın ya da şifrenin oluşturulması, yapılması bu alandaki belirli bir uzmanlık bilgisini gerekli kılsa da bu durum suçun özgü suç haline gelmesine imkan vermez.

Suçun bu alanda uzman bir kişi veya bir bilgisayar korsanı tarafından işlenmesi hali TCK m.61 bağlamında dikkate alınabilir[51].

2. Mağdur

Bazı suçlar bakımından toplumu oluşturan herkes geniş anlamda mağdur olabilir iken, belirli kişiler bu suçların işlenmesiyle münhasır olarak zarar görmüş de olabilirler. Böyle suçlarda toplumu oluşturan herkesin yanı sıra, zarar gören bu kişiler de suçun mağduru olarak kabul edilebilirler[52]. Bu suç bakımından da, bilgisayar programının, şifre veya sair güvenlik kodunun belirli bir kimseye ait olduğu hallerde bu kimselerin suçun mağduru olup olamayacakları tartışılmış olsa da bu görüşe katılamıyoruz. Zira TCK m.245/A ile bilişim suçlarının işlenmesine yönelik hazırlık hareketleri cezalandırılmış durumda olup, henüz daha belirli bir kişiye yönelmiş bir haksızlık gerçekleşmiş değildir[53].

Yukarıda da ifade ettiğimiz gibi, ilgili suç tipi hazırlık hareketlerini cezalandırmaktadır. Henüz bilişim sistemlerine yönelen bir saldırı veya bilişim sistemlerinin araç olarak kullanıldığı bir suç mevcut değildir. Bu nedenle suçun mağduru toplumu oluşturan herkestir[54].

---

50 TUNÇER, s. 1303; KAYA/ÇAKIR, s. 44; ÜNAL, s. 607; AKBULUT, s. 349; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1059. KOCA/ÜZÜLMEZ, **Ceza Özel**, s. 913.

51 ÜNAL, s. 607.

52 TUNÇER, s. 1304; EREN, s. 225-226.

53 TUNÇER, s. 1304; AKBULUT, s. 350.

54 KOCA/ÜZÜLMEZ, **Özel Hükümler**, s. 914. AKBULUT, s. 350.

3. Suçun Konusu

a. Genel Olarak

Tipik hareketin yöneldiği kişi ya da şey, suçun konusunu ifade etmektedir. Eşya veya şahsın fiziki varlığı suçun konusunu oluşturur. Bu suçun konusunu "bilgisayar programı, cihaz, şifre veya sair güvenlik kodu" oluşturur[55].

Bahsi geçen suç tipinin işlenmesiyle herhangi bir zarar veya tehlike ortaya çıkmadığından bu suç tipi soyut tehlike suçu olarak nitelendirilebilir[56]. Soyut tehlike suçlarında suçun konusu bakımından bir tehlikenin oluşup oluşmadığı hakim tarafından araştırılmamaktadır[57]. Hâkim, soyut tehlike suçu açısından tehlikenin somut olarak meydana gelip gelmediğini araştırmıyor olsa da suçun oluşup oluşmadığı hususunda tehlike kaynakları üzerinde bir araştırma yapmalıdır.

TCK m.245/A açısından belirtmek gerekir ki, tek bir güvenlik kodu, şifre veya cihazın suçun konusu olabilmesi mümkündür. Avrupa Siber Suç Sözleşmesi'nin 6. maddesinde, taraf devletlerin bu ve benzeri fiilleri suç sayma yükümlülüğünü yerine getirirken, cihaz, bilgisayar programı, şifre ya da diğer güvenlik kodlarının belirli bir sayıda bulundurulmasının suçun oluşması için bir şart olarak aranabileceği belirtilmiştir[58]. Bununla birlikte bizim kanunumuz açısından, suçun konusu açısından böyle bir sayı sınırlaması getirilmemiştir[59]. Kanımca bu tutum isabetli olmuştur. Burada ilgili cihaz, bilgisayar programı, şifre ya da sair güvenlik kodunun nicelik miktarına bakmaksızın Kanunda bahsedilen suçları işlemeye özgülenmiş olup olmadığına ve ilgili nesnelerin niteliğine bakılarak karar verilmesi gerekir[60].

TCK m.245/A bakımından söyleyecek olursak; ilgili cihaz, program, şifre veya sair güvenlik kodlarının, madde hükmünde belirtilen suçların işlenmesine

---

55 EREN, s. 226; AKBULUT, s. 350; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1057. Doktrinde farklı görüşler de mevcuttur. Örneğin Ünal'a göre, bilgisayar programı, cihaz, şifre veya sair güvenlik kodu fiil araçları olup, suçun konusu bilişim sistemleridir. ÜNAL, s. 608.

56 AKBULUT, s. 349; APAYDIN, Cengiz, **Bilişim Sistemine Girme, Engelleme ve Bozma Suçları**, Seçkin Yayıncılık, Ankara 2023, s. 624.

57 Burada cezalandırmayı haklı gösteren tehlikelilik, hazırlık hareketi ile gelecekte gerçekleşen bir zarar eylemi arasındaki ilişkiden ileri gelmektedir. PUSCHKE, s. 12. (Aktr. ÜNAL, s. 609).

58 EREN, s. 226.

59 EREN, s. 226. Doktrinde ise özellikle depolama ve bulundurma eylemleriyle sınırlı olmak üzere suçun maddi konusuna ilişkin bir sayı şartı getirilmesi önerilmektedir. Bkz. DÜLGER, s. 458.

60 ÜNAL, s. 619. Başka bir görüş de sayı sınırlaması getirilmemesini isabetli bulurken, yalnızca "depolama ve bulundurma" seçimlik hareketleri bakımından bir sayı şartı getirilmesinin şüpheden sanık yararlanır ilkesinin uygulamada gerçekleşmesi bakımından isabetli olacağını belirtmektedir. KARAKURT EREN, s. 226.

elverişli nitelik taşıyıp taşımadığına bakılması gerekir[61]. Nitekim madde gerekçesinde de bu husus özellikle belirtilmiştir: Şayet bulundurulan cihaz, madde hükmünde belirtilen suçları işlemeye elverişli değilse suçun konusunun yokluğundan bahsedilir. Böyle bir durumda işlenemez suç söz konusu olacaktır[62]. Cihazın veya bilgisayar programının bu niteliğinin bulunup bulunmadığı hususunda ise bilirkişi raporu alınması isabetli olacaktır[63].

b. Münhasıran Bilişim Alanında İşlenen Suçlar veya Bilişim Sistemleri Aracılığıyla İşlenebilen Diğer Suçların İşlenmesinde Kullanılmak Üzere Yapılmış ya da Oluşturulmuş Olması

TCK m.245/A düzenlemesinde yer alan suçun konusu, cihaz, bilgisayar programı, şifre veya sair güvenlik kodudur. Burada akla şu soru gelebilir. Peki her cihaz, bilgisayar programı, şifre veya sair güvenlik kodu bu suçun konusunu oluşturabilecek midir yoksa bunların belli bir amaca özgülenmiş olması mı gerekecektir?

TCK m.245/A düzenlemesinde yukarıdaki sorunun cevabı bulunmaktadır. Buna göre, saydığımız nesnelerin bu suçun konusunu oluşturabilmesi için, münhasıran bilişim alanında yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması gerekmektedir. Bu cihaz, bilgisayar programı, şifre veya sair güvenlik kodu başlangıçta kanunun aradığı yasaklı amaçla üretilmiş olmasa bile sonradan bu suçları işlemek amacıyla uyarlanmış ise yine bunlar da suçun konusunu oluşturabileceklerdir[64].

Bununla birlikte TCK m.245/A'nın madde metninde yer alan "*... münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların...*" ifadesinden ne anlaşılması gerektiği doktrinde tartışmalıdır. İlk kısımdan başlayacak olursak: "Münhasıran bu bölümde yer alan suçlar" ifadesinden Türk Ceza Kanunumuzun 10. bölümünde "bilişim alanında suçlar" başlığı altında yer alan suçlar anlaşılmalıdır. Bu husus-

---

61 ÜNAL, s. 609.

62 TEKİN, s. 52.

63 "Tüm dosya kapsamına göre; sanığın olay tarihinde Halk Bankası'na ait ATM'de bulunan kart takma yerine, kart kopyalama aparatı yerleştirdiği, Banka görevlilerinin ihbarı sonucunda sanığın ATM'ye yakın yerde yakalanarak, ATM'ye takılı vaziyette bulunan aparatın kolluk ekibi tarafından çıkartıldığı, sanığa ait cep telefonu ve ATM'ye takılı vaziyette ele geçen aparat üzerinde yapılan inceleme ile alınan Adli Bilirkişi Raporu'na göre, aparatın, ATM cihazına yerleştirilip kartların manyetik şerit bilgilerini kopyalayıp şifrelerini ele geçirmeye yarayan aparat olduğu belirlenmiştir." **Yarg. 8. CD., 06.03.2024, 2555/2170**.

64 EREN, s. 231.

ta bir tartışma zaten bulunmamaktadır. Bununla birlikte madde metninde yer alan "*bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar*" ifadesinden ne anlaşılması gerektiği, esas tartışmalı noktadır.

Öncelikle ifade edelim ki, bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçların hangi suçlar olduğu bizatihi kanun koyucu tarafından ifade edilmiş olsaydı hem kanunilik ilkesi hem de bu tartışmaların önüne geçilmesi bakımından isabetli bir tutum olurdu[65]. Eğer bu ifade geniş bir şekilde yorumlanırsa, bilişim sistemlerinin hayatımızdaki önemi ve bilişim teknolojisindeki hızlı gelişmeler göz önünde bulundurulduğunda, tüm suç türlerinin ileride bilişim sistemleri kullanılarak işlenebileceği sonucu ortaya çıkabilir ve hükmün kapsamı bir anda tüm suçları kapsayacak şekilde genişleyebilir[66]. Ancak bu tür bir yorum, Türk Ceza Kanunu'nun 245/A maddesinin kanunilik ilkesiyle çatışmasına ve özellikle belirlilik ilkesine aykırı bir şekilde uygulanmasına neden olabilecek mahiyet taşıyabilecektir[67]. Bununla birlikte bizim de iştirak ettiğimiz bir başka görüşe göre, hükmü dar yorumlamak ve sadece bilişim sistemlerinin kullanılması suretiyle işlenmeleri suçun nitelikli hali sayılan suçlar[68] ile bu hükmü sınırlandırmak gerekir[69]. Ancak hangi sonuca varılırsa varılsın kanunilik ilkesi bağlamında madde metnindeki belirttiğimiz sorunun giderilmesi gerekmektedir. Kanun koyucunun, bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların hangi suçlar olduğunu açıkça düzenlemesi gerekirdi. Çalışmanın devamında cihaz, bilgisayar programı, şifre ve sair güvenlik kodu terimlerinden ne anlaşılması gerektiğini belirtmeye çalışacağız.

---

65 KORKMAZ, İbrahim, "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla Bulundurulması, İmal ve Ticareti Suçu", **Terazi Hukuk Dergisi**, C. 13, Sa. 142, s. 52.

66 EREN, s. 231. Örneğin doktrinden bir görüş buna yakın bir yorumu benimsemekte ve tehdit, hakaret, şantaj, hırsızlık, dolandırıcılık, zimmet, sahtecilik, haberleşmenin gizliliğini ihlal, kişisel verilerin kaydedilmesi, suç işlemeye tahrik, halkı kin ve düşmanlığa tahrik, müstehcenlik, kumar oynanması için yer ve imkan sağlama, devlet sırlarının ifşası, fikri hakların ihlali gibi çok sayıda suçun bilişim sistemi aracılığıyla işlenmesinin mümkün olduğunu, bu suçların gerçekleştirilmesine yönelik olarak cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun sağlanmasına yönelik olarak gerçekleştirilen fiillerle TCK'nın 245/A maddesinde düzenlenen suçun oluşmasının mümkün olduğunu savunmaktadır. Bkz. GÜL, Doğrudan-Dolaylı Bilişim Suçları, s. 242. Bir başka benzer görüşe göre ise, örneğin, kişisel verilen ele geçirilmesi veya hukuka aykırı olarak kaydedilmesi için cihaz veya bilgisayar programı geliştirilmesi halinde de TCK m.245/A uygulanabilecektir. AKBULUT, s. 354.

67 EREN, s. 231.

68 TCK'da bilişim sistemlerinin kullanılması suretiyle işlenmeleri suçun nitelikli hali olarak düzenlenen suçlar, nitelikli hırsızlık (TCK 142), nitelikli dolandırıcılık (TCK 158), kumar oynanması için yer ve imkan sağlama (TCK 228) suçlarıdır. EREN, s. 231, dn. 45.

69 EREN, s. 231. Krş. ÜNAL, s. 604.

c. Cihaz

Cihaz temel olarak "alet", "aygıt" anlamına gelen bir sözcüktür[70]. TCK ve Sözleşme'de cihaz kavramı tanımlanmış değildir. Cihaz bir donanım unsuruna sahip olan cismani bir varlığı bulunan bir aygıt olarak tanımlanabilir[71]. Cihaz gerektiği zaman bilişim sistemine bağlanabilme veya çıkarılabilme özelliğini haizdir[72]. Bir cihazın bu madde kapsamında suça konu olabilmesi için mutlaka ileri teknoloji gerektiren bir cihaz olması gerekli bir şart değildir[73].

Söz konusu cihazın bu suça konu olabilmesi için bilişim suçlarının veya bilişim sistemlerinin araç olarak kullanılmasıyla işlenen diğer suçların gerçekleştirilmesine özgülenmiş olması gerekmektedir[74]. Bu bağlamda örneğin, ATM cihazlarında kart ya da para sıkıştırmak için kullanılan saç tokası veya basit bir aparat ya da sahte kart üretebilmek için hazırlanan beyaz plastik kartlar bu suçun konusu olamazlar[75]. Maddede yer verilen amaçları gerçekleştirme niteliği taşımayan şeyler yasak cihaz ve programlar suçunun konusunu oluşturmazlar[76].

Yasak kapsamında olan cihazları belirlerken önemli bir sorun olarak çift kullanımlı nesnelerin bu kapsamda değerlendirilip değerlendirilemeyeceği meselesi ile karşılaşılabilir[77]. Nitekim Siber Suç Sözleşmesi taslağı hazırlanırken de bu konu gündeme gelmiş ve cihazların münhasıran ya da spesifik olarak suç işlemek üzere tasarlanmış cihazlarla sınırlı tutulması ve dolayısıyla çift kullanımlı cihazların kapsam dışı bırakılması konusu ayrıntılı olarak tartışılmıştır[78]. Ancak böyle bir düzenlemenin hükmün kapsamını çok fazla daraltacağı ve pratikte uygulanamaz veya çok nadir hallerde uygulanabileceği sorununu doğuracağı endişesiyle bundan vazgeçilmiştir[79]. Bizim Kanunumuz bakımından da çifte kullanımlı cihazların söz konusu olması halinde münhasıran bilişim alanında yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması gereklili-

---

70 https://sozluk.gov.tr/, E.T. 22/12/2024.

71 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1057.

72 ÜNAL, s. 610.

73 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1058.

74 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1058; EREN, s. 227.

75 EREN, s. 227.

76 "sanıklarda ele geçen ATM cihazlarına yerleştirilip kartların manyetik şerit bilgilerini kopyalayıp şifrelerini ele geçirmeye yarayan cihaz ve düzeneklerde" **Yarg. 8. CD., 26/10/2022, 18538/15447.**

77 KAYA/ÇAKIR, s.

78 Explanatory Report to the Convention on Cybercrime, para. 73. https://rm.coe.int/16800cce5b.

79 Explanatory Report to the Convention on Cybercrime, para. 73. https://rm.coe.int/16800cce5b.

ğinden hareket ederek bir sonuca ulaşmak gerekmektedir. Madde metninde kullanılan bu amaç unsuru suçun konusu olabilecek nesneler bakımından sınırlayıcı bir fonksiyon ifa etmektedir.

Aşağıdaki örneklerde ise söz konusu cihazlar bu suçun konusunu oluşturabilecektir. Kibrit kutusu büyüklüğünde olan ve "papağan" olarak da adlandırılan kart okuyucu (*reader*) cihazı sayesinde, kredi kartı veya banka kartı içindeki tüm bilgiler kopyalanabilmekte sahte banka veya kredi kartı üretilmesine zemin hazırlanabilmektedir[80]. Bu cihazla elde edilen kart bilgileri kodlayıcı (encoder) adlı cihazla boş bir kartın arkasındaki manyetik kısma yüklenmekte ve bu sayede sahte banka veya kredi kartları üretilmektedir.

Faillerin sıklıkla başvurduğu bir diğer yöntem de ATM'lerin kart sokulan yerlerine takılan "skimmer" adlı cihazla kart bilgilerini elde etmeleridir[81]. Bu cihazla kartın manyetik şeridindeki bilgiler ele geçirilmektedir. ATM'ye yerleştirilen tuş kaydedici klavye (pinpad) ya da klavyeyi gösteren gizli bir kamera ile de mağdurun şifresi ele geçirilmektedir[82]. Sonucunda TCK m.245'deki suçlar işlenmektedir.

d. Bilgisayar Programları

TCK'da bilgisayar programının tanımına ilişkin bir düzenleme yoktur. Bununla birlikte "5846 sayılı Fikir ve Sanat Eserleri Kanunu'ndaki" düzenleme yol gösterici olabilir. Tanımlar başlığını taşıyan mezkûr düzenlemeye göre bilgisayar programı; "bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmalarını" ifade etmektedir (FSEK 1/B-g)[83].

TCK m.245/A maddesinde bahsi geçen bilgisayar programları ise bilişim sistemlerini çökmesine sebebiyet veren, bilişim sistemlerine hukuka aykırı bir şekilde girilerek verilerin ele geçirilerek başka bir yere transferini sağlayan veya kişinin malvarlığında bir zarar meydana getiren programlardır. Doktrinde bu programlar kötücül yazılımlar olarak adlandırılmaktadır[84]. Kötücül yazılımlar, kullanıcının haberi olmadan veya kullanıcıyı yanıltarak sistemlere bulaşmaktadır[85]. Tıpkı yasaklı cihazlarda olduğu gibi bilgisayar programlarının suçun ko-

---

80 AKBULUT, s. 350.

81 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1058.

82 AKBULUT, s. 350-351.

83 TUNÇER, s. 1308.

84 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1058; Akbulut, s. 351.

85 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1058.

nusu kapsamında olması için suça özgülenmiş olması gerekmektedir[86]. Programın niteliğinde bir suça özgüleme durumu anlaşılamıyorsa uygunsuz kullanım cezai sorumluluk doğurmamalıdır. Bunlara örnek olarak, virüsler, bilgisayar solucanları (*worms*), klavye dinleme sistemleri, tuş kaydediciler, truva atları, casus yazılımlar, mesaj sağanakları, telefon çeviriciler, arka kapılar verilebilir[87].

e. Şifre

Türkçe Bilim Terimleri Sözlüğünde şifre "açık bir metnin karakterlerinin bir algoritma uygulanarak başka karakterlerle yer değiştirilmesi ya da bu karakterlerin sıralarının değiştirilmesi gibi yöntemlere dayanarak metnin içeriğinin gizlenmesi ya da bu işleme tabi tutulmuş metin" şeklinde tanımlanmaktadır[88].

Avrupa Siber Suçlar Sözleşmesi 6. madde hükmünde şifre "bir bilgisayar sisteminin tamamına ya da bir kısmına erişimi mümkün kılan" şeklinde ifade edilmektedir. TCK m.245/A düzenlemesinde şifre kavramı kullanılmış olsa da buna ilişkin bir nitelendirme veya fonksiyon tarifi yapılmadığı için hangi tür şifrelerin suçun konusu kapsamında kalabileceği tartışılmıştı[89]. Belirsizliğin giderilmesi ve hangi tür şifrelerin suçun konusunu oluşturabileceği meselesi bakımından Sözleşmenin 6. maddesinde yer alan tanımdan hareket edilebilir. Buna göre bir bilişim sisteminin tamamına veya bir kısmına erişimi mümkün kılan dijital kilit şeklinde bir anlamlandırma yapılarak şifre kavramının tanımı sınırlandırılabilir[90].

f. Sair Güvenlik Kodu

Türkçe Bilim Terimleri Sözlüğünde "sair güvenlik kodu" teknik bir terim olarak tanımlanmış olmasa da, kod ifadesinin tanımı bulunmaktadır. Bu tanıma göre, kod "bir veri kümesinin tüm öge veya simgelerine bir standarda göre bağlanan sayısal karşılıkların bütünü" anlamına gelmektedir[91].

---

86 ÜNAL, s. 611. Bilgisayar programları bakımından da tıpkı cihazlarda olduğu gibi çifte kullanımlı nesneler sorunu gündeme gelebilir. Yukarıda Sözleşmenin açıklayıcı memorandumunda (73. para.) konunun değerlendirildiğini ve dile getirilen endişeleri belirtmiştik. Bilgisayar programları bakımından bu programın niteliğine bakılması ve Kanunda belirtilen suçları işlemeye özgülenmiş olup olmadığının değerlendirilmesi gerekir.

87 ÜNAL, s. 613; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1059; AKBULUT, s. 352.

88 https://terim.tuba.gov.tr/, E.T. 22/12/2024.

89 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1059. EREN, s. 229.

90 EREN, s. 226.

91 https://terim.tuba.gov.tr/, E.T. 22/12/2024. Sair güvenlik kodu ifadesinin kanunilik ilkesi bağlamında problemli olduğu ileri sürülebilir. Bununla birlikte şifre dışında pek çok farklı nitelikte güvenlik kodunu kapsamına alabilmesi bakımından bu kullanım şeklinin isabetli olduğunu söylemek gerekir. Krş. TUNÇER, s. 1310; ÜNAL, s. 615.

Öğretide sair (diğer) güvenlik kodlarının, bilişim teknolojisi güvenliğini sağlamak amacıyla oluşturulmuş ek kodlar olduğu ifade edilmektedir. Şifre dışında, güvenlik amacıyla kullanılan ses, retina, parmak izi ya da avuç izi tanıma gibi biyometrik özellikler ile kredi kartlarının arka yüzünde bulunan CVC2 ya da CID gibi güvenlik kodları bunlara örnek olarak gösterilmektedir[92].

Tıpkı şifrelerde olduğu gibi sair güvenlik kodlarından hangilerinin yasaklı oldukları ile ilgili bir madde metninde eksiklik söz konusu olsa da, bu eksiklik "bir bilişim sisteminin tamamına veya bir kısmına erişimi mümkün kılan" nitelendirmesinin getirilmesi ile giderilebilecek mahiyettedir[93].

4. Fiil

TCK m.245/A düzenlemesine göre yasaklanan eylemler, "*münhasıran bilişim alanında yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulmasıdır*". Sayılan hareketlerden birinin icrasıyla suç tamamlanmış olacaktır. Bu bağlamda suçun seçimlik hareketli bir suç olduğunu söylemek gerekir. Suç, yalnızca madde metninde sayılan hareketler ile işlenebildiği için aynı zamanda bağlı hareketli bir suçtan bahsetmek gerekir[94]. Ayrıca herhangi bir zarar koşulu aranmadığı için suçun soyut tehlike suçu olduğunu söylemek gerekir[95].

Seçimlik hareketlerden her birisinin aynı konuya yönelmiş olması koşuluyla hareketlerden birkaçının ya da hepsinin icra edilmiş olması suçun da birden fazla oluştuğu anlamına gelmeyecektir[96]. Burada suçun konusunun aynı olup olmadığına bakmak gerekir. Örneğin fail başkasına ait banka veya kredi kartı bilgilerini kopyalamak amacıyla ATM'ye yerleştirmek üzere bir cihaz satın alsa sonra da bu bilgileri boş plastik beyaz kartlara yüklemek üzere bir bilgisayar programı oluştursa bu durumda iki ayrı suçun oluştuğundan bahsetmek gerekir. Zira icra hareketlerinin yöneldiği suçun konusu farklıdır. Bununla birlikte farklı bir örnekte, failin öncelikle yasaklı bilgisayar programını üretmesi sonra da

---

92 DÜLGER, s. 457; AKBULUT, s. 353.

93 EREN, s. 230.

94 KAYA/ÇAKIR, s. 45; AKBULUT, s. 355; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1060.

95 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1060; AKBULUT, s. 355.

96 ÜNAL, s. 616; EREN, s. 233; AKBULUT, s. 355.

bunları satışa arz etmesi halinde artık tek suçun varlığından söz etmek gerekir. Zira suçun konusu tektir[97]. Birden fazla seçimlik hareketin icra edilmesi somut cezanın belirlenmesi bakımından göz önüne alınabilir.

Avrupa Siber Suç Sözleşmesinin 6. maddesine yasaklanan eylemlere baktığımızda ise bunların "üretim, satış, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı veya başka bir şekilde erişilebilir hale getirilmesi" fiilleri olduğunu görmekteyiz. Sözleşmede sayılan seçimlik hareketler, TCK'ya göre daha geniştir. Sözleşmedeki "başka bir şekilde erişilebilir hale getirilmesi" ifadesi hareket unsurunu oldukça genişletmektedir[98]. TCK m.245/A bakımından kanunilik ilkesi bağlamında böyle bir seçimlik harekete yer verilmemesi isabetli olmuştur[99].

Doktrinde seçimlik hareketler arasında "yayma" hareketinin sayılmaması bir eksiklik olarak nitelendirilmiş olsa da[100], sevk etme ve nakletme hareketlerinin "yayma" hareketini de kapsadığı kanaatinde olduğumuzdan bu husus bir eksiklik oluşturmamaktadır[101].

Seçimlik hareketleri sırayla inceleyecek olursak:

İmal etme; bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun kullanılabilir şekilde fiili olarak üretilmesi anlamına gelmektedir[102]. Cihaz, fiziksel varlığı olan işlevsel bir donanım olarak tanımlanır. Bu anlamda, cihazın oluşabilmesi için bileşenlerinin, örneğin kablo veya elektriksel parçalar gibi teknik işlemlerle bir araya getirilerek bağımsız bir şekilde ortaya çıkması gerekmektedir[103]. Cihaz kendini oluşturan parçalardan ayırt edilebilmelidir. Diğer yandan, cihazın parçalarının fail tarafından doğrudan üretilmiş olması zorunlu değildir[104].

Programın, şifre veya sair güvenlik kodunun imal edilmesi de bu suç kapsamındadır. Program, şifre ve sair güvenlik kodunun, cihaz gibi fiziksel bir var-

---

97 ÜNAL, s. 616.

98 StGB m.202c'de de bu fiile aynı şekilde yer verildiğini görmekteyiz.

99 AKBULUT, s. 346.

100 AKBULUT, s. 357.

101 ÜNAL, s. 617.

102 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1060; AKBULUT, s. 355; TUNÇER, s. 1312.

103 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1060.

104 AKBULUT, s. 355; KAYA/ÇAKIR, s. 45; TUNÇER, s. 1312; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1060.

lığı bulunmamaktadır. Yeni bir program imal edilebileceği gibi mevcut bir programın çeşidinin üretilmesi de suç kapsamındadır[105].

İthal etmek, suçun konusunun yurt dışından ülkeye getirilmesi anlamına gelmektedir. Cihazın ithal edilmiş sayılması için doğrudan cihazın kendisinin ithal edilmesi gerekir. Fiziki parçalarının ithal edilip, birleştirilmesi bu seçimlik hareket kapsamında değerlendirilemez[106]. Fiziksel varlığı bulunmayan program, şifre veya sair güvenlik kodunun ithal edilmesinden ise, bunların bir USB bellek ya da hafıza kartı içerisinde taşınarak ülkeye sokulması anlaşılmalıdır[107].

İthal etmenin söz konusu olması için bunların mutlak surette sınır kapısından geçişinin aranması da isabetli değildir. Önemli olan suç konusu olan cihaz, program veya güvenlik kodunun yurt dışından yurt içine aktarılmasıdır. Örneğin yurt dışından bedeli ödenerek internet ortamından indirilmiş bir program da pek tabii bu kapsamda sayılabilecektir[108]. Yurt dışından ithal etmek düzenlenmekle beraber, ihraç etmek düzenlenmediği için bu niteliği taşıyan eylemler sevk etme veya nakletme kapsamında değerlendirilebilir[109].

Sevk etmek fiilinden, suç konusu cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun aracılar vasıtasıyla alıcılara ulaştırılması anlaşılmalıdır[110]. Sevk etme fiilinin yurt içinden veya dışından olmasının bir önemi bulunmamaktadır[111].

Nakletmek ise suça konu cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun bizatihi fail tarafından alıcıya yönlendirilmesi veya teslim edilmesidir[112]. Sevk etme fiilinde aracılar vasıtasıyla ulaştırma hali söz konusu iken, nakletme fiilinde bizzat fail alıcıya ulaştırmaktadır[113]. Bu hareketlerin muhakkak fiziki alanda gerçekleşmesi şart olmayıp, bilişim/ internet alanında da icra edilmesi mümkündür[114].

---

105 ÜNAL, s. 617; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1060.

106 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1060.

107 TUNÇER, s. 1313.

108 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1060; Akbulut, s. 356.

109 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1061.

110 AKBULUT, s. 356.

111 AKBULUT, s. 356.

112 AKBULUT, s. 356.; TUNÇER, s. 1313; ÜNAL, s. 618.

113 ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1061.

114 ÜNAL, s. 618.

"***Depolama ve bulundurma***" seçimlik hareketleri, birbirine yakın anlamlar taşımaktadır. Doktrinde de ifade edildiği üzere aynı veya birbirine çok benzer anlamları taşıyan bu ifadelerin aynı suçta kullanılması isabetli olmadığını söylemek gerekir[115]. Bu seçimlik hareketler, bir cihazın, programın, şifrenin veya sair güvenlik kodunun talep edilmesi durumunda erişilebilecek bir konumda tutulmasını ifade eder. Her iki durumda da, fiili kontrolün söz konusu olduğu bir durumdan bahsedilmelidir. Bu seçimlik hareketler temadi etmektedir. Cihaz, bilgisayar programı, şifre veya sair güvenlik kodu elde bulundurulduğu süre boyunca suç işlenmeye devam etmektedir.

Cihaz bakımından depolama veya bulundurmanın nasıl yorumlanacağı hususunda bir tartışma olmasa da, fiziksel varlığı bulunmayan program, şifre veya sair güvenlik kodu bağlamında hangi eylemlerin depolama veya bulundurma sayılabileceği hususunun tartışılması gerekir. Örneğin program veya şifreyi kaydetme bulundurma sayılacak mıdır? Şüphesiz bu soruya olumlu cevap vermek her ihtimalde mümkün olmayacaktır. Örneğin bulut bilişim alanına yapılan bir kayıt depolama/bulundurma sayılmayabilir[116].

Bir diğer seçimlik hareket ise "***satmak ve satın almaktır"***. Satmak, önceden kararlaştırılan bir meblağ karşılığında cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun alıcıya teslim edilmesidir. Satın almak ise bu saydığımız suçun konusunu oluşturan nesnelerin alınmasını ifade eder[117]. Satışa arz etme ise satmaktan farklı bir fiil olup, suç konusu şeyin satılmasına yönelik bir iradenin ortaya konmasını ifade eder. Bu irade üreticinin satış politikası veya reklamlarıyla ortaya konulabilir. Satışa arz etme de başlı başına cezalandırılmaktadır[118]. Bu seçimlik hareketin gerçekleşmesi için belirli bir alıcının bulunması gerekmez[119].

"Kabul etme", bir bedel ödenmeksizin suç konusu cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun alınması anlamına gelir. Bir diğer seçimlik hareket olan "***başkasına verme"*** de ise bir ücret alınmaksızın suç konusu şeyin başkasına verilmesi anlaşılmalıdır[120].

---

115 ÜNAL, s. 617-618.

116 ÜNAL, s. 618.

117 ÜNAL, s. 618.; KAYA/ÇAKIR, s. 46.

118 ÜNAL, s. 620.

119 TUNÇER, s. 1316.

120 TUNÇER, s. 1315.

Yukarıda TCK m.245/A'da yer alan suçun seçimlik hareketlerini incelemeye ve tanımlamaya çalıştık. Suç bazı seçimlik hareketler bakımından mütemadi bazıları bakımından ise ani suç vasfı taşımaktadır[121]. Örneğin bulundurma ve depolama eylemleri açısından söz konusu hareketlerin icraları devam eden özellik gösterdiği için suç, kesintisiz suç özelliği taşımaktadır, diğer hareketler bakımından ise suçun ani suç özelliği taşıdığını söylemek gerekir[122]. Suçun ani suç mu yoksa mütemadi suç mu olduğu hususu iki açıdan önemlidir. Mütemadi suçlarda, suçun işlenmeye başlandığı yer ve zaman değil, kesintinin gerçekleştiği yer ve zaman dikkate alınır. Bu tespitin önemli bir başka yönü ise iştirak açısından karşımıza çıkar. Mütemadi suçlarda kesintinin gerçekleştiği ana kadar suça iştirak mümkündür.

Dikkat edilecek olursa, suçun oluşumu için kanun koyucu ayrıca bir netice aramamıştır. Suçun oluşumu için madde metninde sayılan seçimlik hareketlerin gerçekleştirilmesi yeterli kabul edilmiştir. Bu bağlamda suç soyut tehlike suçu mahiyetindedir[123].

B. Tipikliğin Manevi Unsurları

Yasak cihaz ve programlar suçu yalnızca kasten işlenebilir. Suçun taksirle işlenmesi mümkün değildir. Tipikliğin tüm maddi unsurları failin bilgisi dahilinde olmalıdır. Fail, cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun bu maddede sayılan suçları işlemek amacıyla oluşturulmuş olduğunu bilmelidir[124].

Suçun oluşumu için kastın yanı sıra failde amaç aranıp aranmayacağı hususu doktrinde tartışmalıdır. Bu tartışmalar, madde metninde yer alan "TCK'nın bilişim alanında işlenen suçlar bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması ya da oluşturulması durumunda" ifadesinden çıkmaktadır. Bir görüşe göre, suçun oluşumu için kastın yanı sıra failde bu yönde bir amaç da bulunması gerektiğinden genel kast değil, özel kast aranır. Üstelik bu yaklaşım Sözleşme'nin 6. maddesi ile de uyumludur. Zira Sözleşme'nin 6. maddesiyle yasa dışı erişim, yasa dışı araya girme, verilere müdahale fiillerinin gerçekleştirilmesinde kullanılmaları amacıyla bilgisayar şifresi, erişim kodu veya benzeri bir verinin ya da söz konusu fiilleri işlemek amacıyla bilgisayar programı dahil tasarlanmış veya

121 EREN, s. 235; DÜLGER, s. 458.

122 EREN, s. 235.

123 EREN, s. 235.

124 TUNÇER, s. 1317.

uyarlanmış cihazın üretimini, satışını, kullanım amaçlı tedarikini, ithalini, dağıtımını veya başka şekilde erişilebilir hale getirilmesini suç haline getirme yükümlülüğü öngörülmüştür[125].

Kanaatimce, suçun oluşum için kastın varlığı yeterli olmayıp, kastın yanı sıra amaç unsurunun da bulunması gerekir. Cihazın, bilgisayar programının, şifre veya sair güvenlik kodunun münhasıran bilişim alanında yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi amacıyla oluşturulması gerekir. Bu kapsamda örneğin bir bankacılık veya sağlık sisteminin güvenlik açığının bulunup bulunmadığının test edilebilmesi gibi meşru bir amaçla bir bilgisayar programının üretilmesi (örneğin sızma testinin yapılması) suç teşkil etmeyecektir[126].

İfade edelim ki kanun koyucunun TCK m.245/A'da suçun manevi unsuru açısından böyle bir amaç unsuruna yer vermesi isabetli olmuştur. Hazırlık hareketlerini cezalandıran soyut tehlike suçlarını sınırlamada amaç veya saik unsuru cezalandırılabilirlik alanının sınırlanması bağlamından önemli bir görev üstlenmektedir[127]. Soyut tehlike suçlarında sıradan bir hareket değil belli bir amaçla gerçekleştirilen hareket cezalandırılmaktadır[128].

Olası kastla işlenip işlenemeyeceği meselesini ele aldığımızda ise, madde metninde amaç unsuruna yer verilmesi dolayısıyla suçun ancak doğrudan kastla işlenebileceğini söylemek gerekir. Suçun olası kastla işlenemeyeceği kanaatindeyiz[129].

Bu suç bakımından kastı kaldıran hata halleri gündeme gelebilecektir. Örneğin bilişim alanında suçları işlemek amacıyla üretilen bir bilgisayar programını bu özelliğini bilmeden indiren bir failin kasten hareket ettiği söylenemez. Düştüğü hata TCK m.30/1 hatası mahiyetindedir. Taksirli şekli de kanunda suç olarak düzenlenmediğinden failin cezai sorumluluğu söz konusu olmayacaktır[130].

---

125 EREN, s. 236. Krş. TUNÇER, s. 1317; ÜNAL, s. 622-623; KAYA/ÇAKIR, s. 47.

126 EREN, s. 237; ÜNAL, s. 621.

127 EREN, s. 235. 623.

128 ÜNAL, s. 622. Hazırlık hareketlerinde hazırlığın subjektif yönüne ilişkin açıklamalar için bkz. YETKİN, s. 439.

129 ARTUK/GÖKCEN/ALŞAHİN/ÇAKIR, Ceza Genel, s. 410; Veli Özer ÖZBEK/ Koray DOĞAN/ Serkan MERAKLI/ Pınar BACAKSIZ/ İsa BAŞBÜYÜK, Türk Ceza Hukuku Genel Hükümler. Seçkin Yayıncılık, 15. Baskı, Y. 2024, s. 127. ÜNAL, s. 623; TUNÇER, s. 1319; EREN, s. 237. Amaç unsuru bulunan suçlarında da olası kastla işlenebileceğine ilişkin farklı görüş için ise bkz. DÜLGER, Murat, Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, 2. Baskı, 2023, s. 467.

130 ÜNAL, s. 623.

C. Hukuka Aykırılık Unsuru

Doktrinde, CMK m.134'te düzenlenen "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" koruma tedbirinin bu suç tipi bakımından görevin ifası veya kanun hükmünü icra (TCK m.24, f.1) kapsamına girdiği belirtilmektedir[131]. Keza sızma testlerinin de görevin ifası hukuka uygunluk sebebi kapsamında kalabileceği belirtilmektedir.

"Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelikte" sızma testinin tanımı şu şekilde yapılmıştır: "Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen güvenlik testleri" sızma testini ifade eder (m.3/1-ğğ).

TCK m.245/A'nın gerekçesinde de "bu tür cihaz ve programların, bilişim güvenliğini test etmek amacıyla yapılmasının veya oluşturulmasının suç oluşturmayacağına" vurgu yapılmaktadır. Bununla birlikte hangi gerekçeyle suç oluşturmayacağına ilişkin bir belirleme madde gerekçesinde bulunmamaktadır[132].

Yukarıda bahsettiğimiz örnekler doktrinde bu suç bakımından gerçekleşmesi muhtemel hukuka uygunluk hallerine örnek olarak verilse de kanaatimce bu örnekler isabetli değillerdir. Bu örneklerde suç oluşmadığı doğrudur ancak gerekçesi yanlıştır. TCK m.245/A'daki suçun oluşması için kanun koyucu failde kastın yanı sıra bir de amaç aramıştır. Buna göre, seçimlik hareketlerin, bilişim alanında suçların ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen suçların işlenmesi amacıyla icra edilmesi gerekir. Oysa yukarıdaki ihtimallerde delil elde etmek veya güvenlik açıklarını test edebilmek gibi meşru amaçlarla bilgisayar programı veya cihazlar kullanılmaktadır. Bu nedenle ilgili fiillerin suç oluşturmaması hukuka uygunluk nedeninden yararlandıkları için değil, amaç unsuru bulunmadığı içindir. Bahsedilen fiiller tipe uygun değildir[133].

V. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

A. Teşebbüs

Yasak cihaz ve programlar suçu, bulundurma veya depolama şeklindeki seçimlik hareketleri hariç sırf hareket suçu mahiyetindedir[134]. Sırf hareket suçla-

---

131 KOCA/ÜZÜLMEZ, **Özel Hükümler**, s. 915.

132 ÜNAL, s. 625.

133 EREN, s. 238; ÜNAL, s. 626. Krş. TUNÇER, s. 48.

134 ÜNAL, s. 627. Hazırlık kaynaklı ceza sorumluluğunda teşebbüs sorununa ilişkin görüşler için (şekli bakış açısıyla hareket eden görüşler-maddi bakış açısıyla hareket eden görüşler) bkz. YETKİN, s. 464, 479. Hazırlık kaynaklı ceza sorumluğunda teşebbüse ilişkin değerlendirme için bkz. YETKİN, s. 489.

rında, suçun oluşması için kanuni tarifte yer alan hareketin yapılması yeterli olup, ayrıca dış dünyada bir değişikliğin meydana gelmesi gerekmez. Sırf hareket suçlarında teşebbüs ancak hareketin kısımlara bölünebildiği durumlarda mümkündür[135].

Bu bilgiler ışığında yasak cihaz ve programlar suçunu oluşturan seçimlik hareketlerden bölünebilir nitelikte olanlar bakımından suça teşebbüs söz konusu olabilir. Temadi özelliği gösteren bulundurma veya depolama seçimlik hareketlerinde ise suça teşebbüs ancak ele geçirme anına kadar mümkündür[136]. Fail, suça konu cihaz, program, şifre veya sair güvenlik kodunu kendi egemenlik alanına geçirmesiyle suç tamamlanmış olacaktır olup failin elinde bulundurduğu veya depoladığı süre dahilince suç işlenmeye devam edecektir[137].

Örneğin bilişim alanında suçları işlemekte kullanmak üzere bir cihazın imaline başlanmış ancak polis baskını yapılması nedeniyle imalat yarıda kalmış ise teşebbüs hükümlerinden söz etmek gerekecektir[138].

Seçimlik hareketler arasında yer alan satma ve satışa arz etme eylemleri açısından ise suçun teşebbüse elverişli olduğunu söylemek zordur. Bir kere satışa arz etme fiili zaten arz ettiği özellik itibariyle teşebbüs niteliğinde bir hareket olup; kanun koyucu suç tanımında yaptığı tercihle bu hareketin tamamlanmış suç gibi cezalandırılacağını hükme bağlamıştır[139]. Satışa arz etme fiili teşebbüs suçu olduğundan ayrıca teşebbüse elverişli değildir. Satma seçimlik hareketi bakımından da suç teşebbüse elverişli değildir. Zira satma eylemi bakımından teşebbüs kapsamında değerlendirilebilecek olan hareketler zaten satışa arz etme oluşturacağından satma hareketi bakımından da suç teşebbüse elverişli değildir[140].

TCK m.245/A "yasak cihaz ve programlar suçuna" teşebbüs yukarıda açıklanan konular bağlamında mümkün olabileceğinden, bu suç bakımından gönüllü

---

135 TUNÇER, s. 1322. AKBULUT, s. 359 vd.; DÜLGER, s. 459; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1035; KOCA/ÜZÜLMEZ, **Ceza Hukuku Özel Hükümler**, s. 915; KORKMAZ, s. 53. Bununla birlikte, TCK m.245/A düzenlemesi zaten hazırlık hareketi niteliğindeki eylemleri cezalandırdığı için yasak cihaz ve programlar suçuna teşebbüsü mümkün görmeyen bir görüş de bulunmaktadır. GÜL, s. 350. Hazırlık suçlarına teşebbüsün kabul edilmesi, zaten öne alınmış ceza sorumluluğunun bir kez daha ve neticede aşırı derecede genişletilmesi anlamına gelir şeklindeki görüş için bkz. YETKİN, s. 489 vd.

136 ÜNAL, s. 627.

137 ÜNAL, s. 627.

138 AKBULUT, s. 360; KOCA/ÜZÜLMEZ, **Türk Ceza Hukuku Özel Hükümler**, s. 915; DÜLGER, s. 459; KORKMAZ, s. 53. EREN, s. 240.

139 TUNÇER, s. 1323; EREN, s. 240.

140 EREN, s. 241. Ayrıca bkz. KAZAKER BOZKURT, s. 264; ÜNAL, s. 622; YETKİN, s. 135 vd.

vazgeçme hükümleri de uygulanabilir mahiyettedir[141]. Örneğin mobil bankacılık uygulaması üzerinden başkasına ait kredi kartı bilgilerini kopyalamak amacıyla bir program yazmaya başlayan kişi sonradan kendi iradesiyle bundan vazgeçerse hakkında gönüllü vazgeçme hükümleri uygulanır ve teşebbüsten cezalandırılmaz.

TCK m.245/A hükmünde failin etkin pişmanlıktan yararlanabileceğine ilişkin bir düzenleme mevcut olmamakla birlikte, olması gerektiğine ilişkin birtakım görüşler vardır. Örneğin failin kredi kartı kopyalama cihazlarını (*skimmer*) satın aldıktan sonra daha sonra pişmanlık duyarak kolluk kuvvetlerine bu cihazları teslim etmesi halinde hakkında etkin pişmanlık hükümleri uygulanabilecek midir[142]? TCK m.245/A'ya benzer bir düzenleme olan, "para ve kıymetli damgaları yapmaya yarayan araçlar" da sahteciliği konu alan fiillerin etkin pişmanlık düzenlemesi TCK m.201'de[143] düzenlenmiş iken TCK m.245/A'da yer alan yasak cihaz ve programlar suçunda bir etkin pişmanlık düzenlemesinin bulunmaması doktrinde eleştirilmektedir[144]. TCK m.201/2 hükmüne benzer şekilde TCK m.245/A bakımından da bir etkin pişmanlık hükmünün getirilmesi önerilmektedir[145]. İfade edelim ki bu eleştiriler haklıdır.

B. İştirak

TCK m.245/A'da yer alan düzenleme iştirak bakımından herhangi bir özellik arz etmez[146]. Maddede yer alan, satma ve satın alma, başkalarına verme ve

---

141 KOCA/ÜZÜLMEZ, **Ceza Özel**, s. 915. "Örneğin, failin bu suça özgülenen bir cihazı satın almak istemesi ve daha sonra bundan vazgeçmesi halinde hakkında cezaya hükmolunmayacaktır. Zira suçun tamam olan kısmı herhangi bir suç oluşturmamaktadır." Örnek için bkz. ÜNAL, s. 627.

142 ÜNAL, s. 628.

143 Etkin pişmanlık

Madde 201- (1) "Sahte olarak para veya kıymetli damga üreten, ülkeye sokan, nakleden, muhafaza eden veya kabul eden kişi, bu para veya kıymetli damgaları tedavüle koymadan ve resmi makamlar tarafından haber alınmadan önce, diğer suç ortaklarını ve sahte olarak üretilen para veya kıymetli damgaların üretildiği veya saklandığı yerleri merciine haber verirse, verilen bilginin suç ortaklarının yakalanmasını ve sahte olarak üretilen para veya kıymetli damgaların ele geçirilmesini sağlaması halinde, hakkında cezaya hükmolunmaz. (2) Sahte para veya kıymetli damga üretiminde kullanılan alet ve malzemeyi izinsiz olarak üreten, ülkeye sokan, satan, devreden, satın alan, kabul eden veya muhafaza eden kişi, resmi makamlar tarafından haber alınmadan önce, diğer suç ortaklarını ve bu malzemenin üretildiği veya saklandığı yerleri ilgili makama haber verirse, verilen bilginin suç ortaklarının yakalanmasını ve bu malzemenin ele geçirilmesini sağlaması halinde, hakkında cezaya hükmolunmaz".

144 ÜNAL, s. 628.

145 ÜNAL, s. 629.

146 Bununla birlikte doktrinde farklı görüşler de vardır. Örneğin, Yetkin'e göre hazırlık suçlarında iştirak konusunu değerlendirirken, iştirak hükümlerinin cezalandırılabilirliği genişleten düzenlemeler olduğu gerçeği temel alınmalıdır. Bu açıdan bakıldığında, hazırlık suçlarına teşebbüs ile iştirak arasında bir ben-

kabul etme gibi seçimlik hareketler bakımından suçun çok failli bir suç özelliği gösterdiğini söylemek gerekir[147]. Bu gibi hallerde satan, satın alan, başkasına veren veya kabul eden kişilerin her biri fail olarak sorumlu tutulacaktır[148].

Bu suç dolaylı faillik şeklinde de karşımıza çıkabilir. Örneğin A, C'ye iletmesi için, B'ye ürettiği kredi kartı kopyalama cihazını verse ve cihazın bu özelliğini B'ye söylemese, B de bu cihazı gidip, C'ye teslim etse... Bu ihtimalde faillerin cezai sorumluluğu nasıl belirlenecektir? Burada A yasaklı cihazı naklederken B'yi araç olarak kullanmıştır. B'yi cihazın yasaklı olduğu hususunda hataya düşürmek suretiyle A, arka plandaki kişi olarak dolaylı fail konumundadır. B ise cihazın yasak cihaz kapsamında olduğunu bilmediğinden bu hatasından (TCK m.30/1) yararlanacak ve herhangi bir sorumluluğu olmayacaktır. C ise yasak cihazı kabul ettiği için, TCK m.245/A'dan sorumlu olacaktır.

Madde metnine bakıldığında normalde azmettirme kapsamında değerlendirilebilecek bazı eylemlerin (örn. satışa arz etme gibi) seçimlik hareket olarak düzenlendiği görülmektedir. Böyle bir ihtimalde ilgili kişiler azmettiren veya yardım eden sıfatıyla değil, fail olarak suçtan sorumlu olacaklardır[149].

TCK m.245/2'de düzenlenen sahte banka veya kredi kartı üretme suçuyla ilişkisi bakımından iştirak konusu gündeme gelebilir. Örneğin sahte kredi kartı üretme faaliyeti iştigal eden B'ye, bu eylemini icra ederken kullanacağı cihazları temin eden A suça iştirak kuralları çerçevesinde nasıl sorumlu tutulacaktır? Normalde sahte kredi kartı üretme eylemine uygun cihazları temin eden kişi TCK m.245/2'ye yardım eden sıfatıyla sorumludur. Ancak TCK m.245/A düzenlemesi, bizatihi kişinin bu eyleminden fail olarak sorumlu tutulmasını gerektirmektedir. "Failliğin şerikliğe asliliği" kuralı gereğince bu durumda A'nın TCK m.245/A'dan sorumluluğuna gitmek gerekecektir[150].

Bazı ihtimallerde ise müşterek faillik şeklinde de suçun işleniş şekli karşımıza çıkabilecektir. Örneğin A, başkasına ait kart bilgilerini kopyalamak için bir cihaz üretse sonra da bu cihazı B'ye satsa, B'de bunu banka ATM'sine yerleştirip başkalarının kart bilgilerini elde edip sonra sahte kredi kartı üretse ve

zerlik bulunmaktadır. Bu doğrultuda, hazırlık suçlarına teşebbüste olduğu gibi, iştirak de hazırlık suçları kapsamında cezalandırılamaz sonucuna varılmalıdır. söz konusu hazırlık eylemine teşebbüs edilmesi ya da bu eyleme yardım veya azmettirme fiillerinin cezalandırılmaması gerekir. Çünkü hazırlık suçlarına teşebbüs veya iştirak, cezai anlamda bir haksızlık niteliği taşımamaktadır. YETKİN, s. 498-499.

147 KOCA/ÜZÜLMEZ, **Ceza Özel**, s. 916; KORKMAZ, s. 53.

148 EREN, s. 241; TUNÇER, s. 1324; ÜNAL, s. 629.

149 TUNÇER, s. 1324.

150 EREN, s. 241. Krş. TUNÇER, s. 1324.

sonra bu kartla elde ettiği kazançtan A'ya belli bir pay verse, faillerin cezai sorumlulukları nasıl belirlenecektir? Burada A ve B hem TCK m.245/A'dan hem de TCK m.245/2 ve TCK m.245/3'ten müşterek fail olarak sorumlu olacaklardır. Burada suçun işlenişine katılan suç ortaklarının hedef suç bakımından da iştirak iradelerinin olduğunu gözden kaçırmamak gerekecektir.

C. İçtima

TCK m.245/A'da yer alan suçun zincirleme suç şeklinde işlenmesi mümkündür. Bu bağlamda bir suç işleme kararı kapsamında değişik zamanlarda birden fazla kez aynı suçun işlenmesi halinde faile tek bir suçtan ceza verilir ancak cezası dörtte birinden dörtte üçüne kadar artırılır[151]. Suçun mağduru belli bir kişi değil, toplumu oluşturan herkes olduğundan, aynı neviden fikri içtima hükmünün bu suç bakımından uygulanması ise mümkün değildir[152].

TCK m.245/A düzenlemesi yukarıda da ifade olunduğu üzere hazırlık hareketlerini cezalandıran bir normdur[153]. Bu nedenle bu suç tipi bakımından araç suç/amaç suç ilişkisi gündeme gelebilir[154]. Örneğin failin sahte banka veya kredi kartı üretmek amacıyla bir kart kopyalama cihazı (skimmer) temin etmesi sonrasında bu cihazı kullanarak sahte bir kredi kartı üretmesi ve en sonunda da bu kartı kullanarak haksız yarar temin etmesi halinde cezai sorumluluğu nasıl belirlenecektir?

Hazırlık hareketlerinin bağımsız suç olarak kabul edildiği hallerde fail hazırlık hareketlerini icra ettikten sonra bir de amaç suçun icrasına girişirse artık sadece hedef suçtan sorumlu tutulması gerekir, hazırlık hareketini bağımsız olarak cezalandıran normdan dolayı ayrıca sorumlu tutulmamalıdır[155]. Doktrinden Sarıtaş'ın verdiği bir örneğe göre, Türk Ceza Kanunu'nun 197. maddesinde parada sahtecilik suçunu düzenleyen kanun koyucu, 200. maddede ise "paralarla kıymetli damgaların üretiminde kullanılan alet veya malzemeyi izinsiz olarak üreten, ülkeye sokan, satan, devreden, satın alan, kabul eden veya muhafaza eden" kişiyi cezalandırarak, aslında parada sahteciliğe yönelik hazırlık hareket-

---

151 KOCA/ÜZÜLMEZ, Ceza Özel, s. 916; ÖZBEK/DOĞAN/BACAKSIZ, **Türk Ceza Hukuku Özel Hükümler**, s. 1035; DÜLGER, s. 460; KORKMAZ, s. 53; ÜNAL, s. 630.

152 EREN, s. 242.

153 TEZCAN, Durmuş/ERDEM Mustafa Ruhan/ÖNOK, R. Murat, **Teorik ve Pratik Ceza Özel Hukuku**, Güncellenmiş 21. Baskı, Eylül 2023, Seçkin Yayıncılık, Ankara, s. 1082.

154 ÜNAL, s. 630.

155 SARITAŞ, Erkan, "Cezalandırılmayan Önceki Hareketler", **İstanbul Hukuk Mecmuası**, C. 80, Sa. 2, s. 637. Hazırlık suçu-hedef suç arasında talilik ilişkisi olduğuna dair görüş için bkz. YETKİN, s. 514-516.

lerini bağımsız bir suç olarak tanımlamıştır. Bu bağlamda, fail sahte para üretme amacıyla bu işe yarayan aletleri izinsiz olarak satın alır ve bu aşamada yakalanırsa, TCK m.200 kapsamında sorumlu tutulacaktır[156]. Ancak, bu aletleri kullanarak sahte para basmaya yönelik elverişli hareketlerde bulunursa, artık yalnızca TCK m.197 uyarınca cezalandırılacak, ayrıca TCK m.200 kapsamında sorumlu tutulmayacaktır[157].

Bu bağlamda yukarıda verdiğimiz örneği çözümleyecek olursak: Failin sahte bir kredi kartı üretmek amacıyla yasak bir cihaz *(skimmer)* satın alması, sonrasında bu cihazı kullanarak sahte bir kart üretmesi ihtimalinde TCK m.245/A ile TCK m.245/2 arasında araç suç/amaç suç ilişkisi söz konusu olduğundan artık failin yalnızca hedef suçtan yani TCK m.245/2'den cezalandırılması gerekir. TCK m.245/A hazırlık normu olduğu için failin bundan doğan sorumluluğuna gidilemeyecektir[158].

Bazı hallerde ise bu suçun özel kanunlarda düzenlenen benzer suçlarla içtima ilişkisi de gündeme gelebilir. Örneğin "Elektronik İmza Kanununun 16.

---

156 SARITAŞ, s. 638.

157 SARITAŞ, s. 638. Yazarın eserinde verdiği bir başka örnek de konu bakımından aydınlatıcı ve önemlidir. Örneğin, bir kişi hukuka uygun şekilde erişim sağladığı bir bilişim sistemine, yetkisi olmamasına rağmen veri yerleştirebilir. Ancak, çoğu durumda bu fiilin gerçekleştirilebilmesi için öncesinde bilişim sistemine hukuka aykırı olarak girilmesi gerekir. Bu tür durumlarda, fail amacına ulaşmak için önce bilişim sistemine giriş yapmış, ardından sisteme veri yerleştirmişse, yalnızca hedef suçtan sorumlu tutulacak, ayrıca öncü suçtan dolayı cezalandırılmayacaktır. Dolayısıyla, bilişim sistemine veri yerleştirmek amacıyla hukuka aykırı şekilde sisteme girildiği hallerde, TCK m.243/1 hükmü, TCK m.244/2 karşısında uygulanmayacak ve fail yalnızca ikinci suç nedeniyle cezalandırılacaktır. Açıklamalar için bkz. SARITAŞ, s. 638-639.

158 Tüm dosya kapsamına göre; sanığın olay tarihinde Halk Bankası'na ait ATM'de bulunan kart takma yerine, kart kopyalama aparatı yerleştirdiği, Banka görevlilerinin ihbarı sonucunda sanığın ATM'ye yakın yerde yakalanarak, ATM'ye takılı vaziyette bulunan aparatın kolluk ekibi tarafından çıkartıldığı, sanığa ait cep telefonu ve ATM'ye takılı vaziyette ele geçen aparat üzerinde yapılan inceleme ile alınan Adli Bilirkişi Raporu'na göre, aparatın, ATM cihazına yerleştirilip kartların manyetik şerit bilgilerini kopyalayıp şifrelerini ele geçirmeye yarayan aparat olduğu belirlenmiştir. Sanığın cep telefonunda ve ele geçen aparat da herhangi bir kişiye ait bilgi veya kopyalanmış kart bilgilerinin bulunmadığının tespit edilmesi karşısında; sanığın eyleminin 5237 sayılı Kanun'un 136 ncı maddesi kapsamında değerlendirilemeyeceği ancak; sanığın eylemine uyan 5237 sayılı Kanun'un 245 inci maddesinin A bendinde düzenlenen yasak cihaz (Aparat) veya programlar bulundurma suçundan mahkumiyeti yerine, yasal ve yerinde olmayan gerekçe ile yazılı şekilde beraat hükmü kurulması, hukuka aykırı bulunmuştur." **Yarg. 8. CD., 06/03/2024, 2555/2170.** İncelemeye konu olay; sanıklar ... ve ... ile soruşturma aşamasında yakalanamadığı için hakkında tefrik kararı verilen Doğan Keskin'in, fikir ve eylem birliği içerisinde iştirak halinde kart kopyalama aparatını Erzurum ilinde bulunan Vakıfbank ATM'lerine yerleştirdikleri, mağdurlara ait bankamatik kartlarını kopyalayarak, İstanbul'daki ATM'de mağdurların kartlarından bilgileri ve rızaları dışında para çekilmesi suretiyle, sanıkların sahte kredi kartı üretme, sahte banka veya kredi kartı kullanmak suretiyle yarar sağlama, yasak cihaz veya programlar suçlarını işledikleri, iddiasına ilişkindir... Sanıklar hakkında sahte kredi kartı üretme ve yasak cihaz veya programlar suçlarından kurulan hükümler yönünden Gerekçe bölümünün (A) bendinde açıklanan nedenlerle Erzurum Bölge Adliye Mahkemesi 4. Ceza Dairesi'nin, 2018/1191 Esas, 2018/991 Karar ve 25.05.2018 tarihli kararına yönelik sanık ... müdafiin ve sanık ... müdafiin temyiz istemlerinin, 5271 sayılı Kanun'un 298 inci maddesinin birinci fıkrası uyarınca, Tebliğname'ye uygun olarak, oy birliğiyle REDDİNE" **Yarg. 8. CD., 03/04/2024, 12713/3010**.

maddesinde yer alan imza oluşturma verilerinin izinsiz kullanımı suçu" ile "koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçu"nun yer aldığı Fikir ve Sanat Eserleri Kanunu'nun 72. maddesi ve "telsiz cihaz ve sistemlerini izinsiz şekilde satma, işletme ve kullanma suçu"nun düzenlendiği Elektronik Haberleşme Kanunun 63. maddesinin 4. fıkrası özel hüküm olarak karşımıza çıkabilir. Bu gibi hallerde soruna görünüşte içtima kurallarından özel norm-genel norm ilişkisi bağlamında yaklaşılmalı ve özel kanunlardaki hükümlerin özel normun önceliği kuralı kapsamında uygulanması cihetine gidilmelidir. Böyle bir halde genel hüküm mahiyetinde olan TCK m.245/A düzenlemesinin uygulanma ihtimali bulunmamaktadır[159].

VI. YAPTIRIM, SORUŞTURMA VE KOVUŞTURMA

TCK m.245/A maddesinde belirtilen suçun yaptırımı "bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası" olarak öngörülmüştür. Doktrinde bu suçun hazırlık hareketlerini cezalandıran bir norm olmasına rağmen yaptırım miktarının yüksek olduğu dile getirilmektedir[160]. TCK m.245/A hükmünün cezası, bilişim suçlarından yalnızca TCK m.244/4 ve m.245 hükümlerine göre daha az olup, diğer suçlarla ise birbirine yakındır[161]. Hedef suçlara nazaran TCK m.245/A'nın haksızlık içeriği daha az olduğundan ceza miktarının azaltılması gerekir[162]. Bu kapsamda bu suç açısından hapis ve adli para cezası miktarı azaltılabilir. Bu haliyle hazırlık suçlarında cezanın soyut olarak belirlenmesine ilişkin ilkelerle uyum göstermemektedir[163].

Suçun işlenmesiyle tüzel kişi lehine haksız bir menfaat sağlanmışsa TCK m.246 hükmü uyarınca tüzel kişiye özgü güvenlik tedbirlerinin uygulanması gündeme gelebilecektir.

Suçun mağduru toplumu oluşturan herkes olduğundan takibi şikayete bağlı bir suç değildir. Takibi re'sen yapılan suçlardandır. 5235 sayılı "Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun" 11. ve 12. maddeleri uyarınca bu suçu yargılamakla görevli mahkeme asliye ceza mahkemesidir. Hakimler ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1299 sayılı kararı uyarınca ihtisaslaşmanın sağlanması ama-

159 KOCA/ÜZÜLMEZ, **Özel Hükümler**, s. 963; AKBULUT, s. 361, KAYA/ÇAKIR, s. 51; ÜNAL, s. 631.

160 ÜNAL, s. 632; KAYA/ÇAKIR, s. 49.

161 YETKİN, s. 582-583.

162 YETKİN, s. 583.

163 YETKİN, s. 583.

cıyla sayılan mahkemelerin bazı daireleri bilişim suçlarına bakmakla yükümlü kılınmışlardır[164]. Bu kapsamda örneğin asliye ceza mahkemesinin görev alanına giren suçlar yönünden; a) İki asliye ceza mahkemesi bulunan yerlerde 2 numaralı, b) Üç, dört veya beş asliye ceza mahkemesi bulunan yerlerde 3 numaralı, c) Altı, yedi, sekiz veya dokuz asliye ceza mahkemesi bulunan yerlerde 6 numaralı, d) On veya daha fazla (yirmi beşten az) asliye ceza mahkemesi bulunan yerlerde 8 numaralı, e) Yirmi beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20 ve 21 numaralı, f) Otuz beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20, 21 ve 22 numaralı asliye ceza mahkemelerinin bakmasına karar verilmiştir. İhtisaslaşmanın sağlanması adına alınan bu karar isabetli olmuştur.

SONUÇ

Avrupa Konseyi Siber Suç Sözleşmesinin "cihazların kötüye kullanılması" başlıklı 6. maddesinde taraf devletlere, bilişim suçlarıyla ilgili hazırlık hareketlerinin ceza normuyla karşılanması hususunda bir yükümlülük yüklenmiştir. Ülkemiz de Sözleşmeye taraf olmanın bir gereği olarak ceza kanunumuzda bu fiilleri suç olarak ihdas etmiş ve kanun koyucu, 24/03/2016 tarihli ve 6698 sayılı Kanun ile birlikte TCK'ya 245/A maddesini eklemiştir. Bu düzenlemenin yapılmasıyla Sözleşmede öngörülen yükümlülük yerine getirilmiştir.

Hazırlık hareketlerinin cezalandırılabilir eylemler olup olmaması gerektiği hususunda doktrinde oldukça farklı görüşler bulunmaktadır. Kanaatimce, kural olarak hazırlık hareketlerinin cezasızlığı, istisnai hallerde hazırlık hareketlerinin cezalandırılması düşüncesi ön planda olmalıdır. Bununla birlikte bazı hallerde uluslararası Sözleşmelerde bu durum bir yükümlülük olarak taraf devletlere yüklenebilir. Siber Suç Sözleşmesine taraf bir ülke olarak bilişim suçlarında hazırlık hareketlerinin cezalandırılmasına ilişkin yükümlülüğün yerine gelmesi bakımından TCK m.245/A önemlidir.

Suçun düzenlendiği madde başlığının "yasak cihaz veya programlar" olarak belirlenmesinin doğru bir tercih olmadığı belirtilmektedir. Madde başlıklarının seçiminde fiil unsurunun ön plana çıktığı, oysa TCK m.245/A bakımından su-

[164] 30.11.2021 tarih, RG: 31675. "Ağır ceza ve asliye ceza mahkemelerine gelen işlerin vasıf ve mahiyeti itibarıyla çeşitli olması, bu çerçevede bilişim ile ilgili suçlardan kaynaklanan dava ve işlerin niteliklerinin farklı olması göz önünde bulundurularak, gerek uygulama birliğinin sağlanması, gerekse etkinlik ve verimliliğin artırılması ile ihtisaslaşmanın önemi nazara alınarak, mezkûr dava ve işlerde iş dağılımı bakımından iki veya daha fazla dairesi bulunan mahallerde ihtisaslaşmaya gidilmesinde fayda olacağı değerlendirilmiştir". Hâkimler ve Savcılar Kurulu Kararı, 25/11/2021 tarihli ve 1229 sayılı kararı.

çun konusu olan unsurlara madde başlığında yer verildiği bundan dolayı madde başlığının madde içeriği ile uyuşmadığı, içeriği yansıtmadığı ileri sürülmektedir. Bizde bu eleştirilere katılmaktayız. Kanaatimce madde başlığı "cihaz veya programların kötüye kullanılması" veya "yasak cihaz veya programların üretilmesi veya ticareti suçu" şeklinde değiştirilebilir.

Suç seçimlik hareketli bir suçtur. Aynı konuya yönelmiş olmak koşuluyla seçimlik hareketlerden bir tanesinin yapılması suçun oluşumu bakımından yeterlidir. Birden fazla seçimlik hareketin icra edilmesi suçun da birden fazla işlendiği anlamına gelmez.

Avrupa Konseyi Siber Suç Sözleşmesi ile kıyasladığımızda, TCK m.245/A'nın büyük ölçüde Sözleşme ile paralellik taşıdığını söylemek gerekir. Bununla birlikte farklılaştığı noktalar da yok değildir. Örneğin fiil unsuru açısından baktığımızda Sözleşme'nin kapsamının daha geniş olduğunu, belirlilik ilkesi bağlamında değerlendirdiğimizde TCK'da yer alan düzenlemenin sınırlarının daha belirli olduğunu söylememiz gerekir. Bununla birlikte Kanun'daki düzenlemenin önemli bazı sorunlu noktaları da bulunmaktadır. Örneğin madde metninde kullanılan 'bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar' ifadesi kanunilik ilkesi bağlamında problemli noktalardan bir tanesidir. Bu ifadeden kastedilen suçlar hangi suçlardır? İkinci olarak suçun oluşumu bakımından yasak cihaz ve programlar bakımından herhangi bir sayı sınırının aranıp aranmayacağı ve ayrıca çift kullanım özelliği gösteren (dual use) nesnelerin bu kapsamda değerlendirilip değerlendirilemeyeceği kanunilik ilkesi bağlamında problemli diğer noktalardır.

TCK m.245/A'nın madde metninde yer alan "*... münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların...*" ifadesinden ne anlaşılması gerektiği doktrinde de tartışmalıdır. Kanaatimce hükmü dar yorumlamak ve bilişim alanında suçlar ile bilişim sistemlerinin kullanılması suretiyle işlenmeleri suçun nitelikli hali sayılan suçlar ile bu hükmü sınırlandırmak ve hükmü bu şekilde yorumlamak gerekir. Aksi takdirde TCK m.245/A'nın kapsamı bir anda tüm suçları kapsayacak bir hazırlık suçuna dönüşebilir.

Siber Suç Sözleşmesinin ilgili hükmü gereğince (m.6/1-b) taraf devletler, bilişim suçlarında hazırlık hareketlerinin cezalandırılması hususunda yasal düzenleme yaparken bahsi geçen öğelerden belirli bir sayıda bulundurmayı suçun oluşumu bakımından şart koşabileceklerdir. Sözleşme, taraf devletlere kendi ulusal mevzuatları bakımından böyle bir inisiyatif tanımıştır. Bizim Kanununuz ise TCK m.245/A'da sayılan öğeler bakımından suçun oluşumu için herhangi

bir sayı sınırlaması getirmemiştir. Suçun oluşumu bakımından burada cihaz, bilgisayar programı, şifre veya güvenlik kodunun belli bir sayıya ulaşıp ulaşmadığını araştırmaya gerek bulunmamaktadır. Suçun oluşumu bakımından gözden kaçırılmaması gereken önemli nokta ise bunların niteliğine ve bilişim alanında suçları veya bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçları gerçekleştirmeye elverişli olup olmadığını bakılarak karar verileceği gerçeğidir.

Benzer bir durum çift kullanım (dual use) özelliği gösteren nesneler için de söz konusudur. Üstelik bu tartışma Sözleşmenin açıklayıcı raporunda da gündeme gelmiştir. Çift kullanımlı nesnelerin doğrudan kapsam dışı bırakılmasının uygulamayı tıkayacağı ve hükmü uygulanamaz hale getirebileceği endişesiyle Sözleşme'de buna yer verilmemiştir. Başlangıçta hukuka uygun bir amaçla üretilen bir cihaz veya bilgisayar programı sonradan bilişim alanında suçları işlemek amacıyla geliştirilebilir veya güncellenebilir. Bu durumda bunlar da pek tabii bu suçun konusunu oluşturabileceklerdir.

Hakem Değerlendirmesi : Dış bağımsız.
Çıkar Çatışması **:** Yazar çıkar çatışması bildirmemiştir.
Finansal Destek **:** Yazar bu çalışma için finansal destek almadığını beyan etmiştir.
Peer-review ***: Externally peer-reviewed.***
Conflict of Interest ***: The author has no conflict of interest to declare.***
Grant Support ***: The author declared that this study has received no financial support.***

KAYNAKÇA

AKBULUT, Berrin, **Bilişim Alanında Suçlar**, 2. Baskı, Adalet Yayınevi, Ankara, 2017.

ALİUSTA, Cahit/BENZER, Recep, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, C. 4, No, 2, 2018.

ARTUK, Mehmet Emin/GÖKCEN, Ahmet/ALŞAHİN, M. Emin/ÇAKIR, Kerim, **Ceza Hukuku Genel Hükümler**, Adalet Yayınevi, 18. Baskı, 2024.

ÇEKEN, Hüseyin, "Amerika Birleşik Devletlerinde İnternet Yolu ile İşlenen Suçlara İlişkin Düzenlemeler", **Askeri Adalet Dergisi**, Sa: 144, Y. 2002.

DURSUN, Selman, "İnternetten Kaynaklanan Ceza Sorumluluğundaki Gelişmeler", **Mhb**, Prof. Dr. Ünal Tekinalp'e Armağan, C. 3, Sa: 1-2, 2003.

DÜLGER, Murat Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku**, Genişletilmiş ve Güncellenmiş 8. Baskı, Seçkin Yayıncılık, İstanbul, 2020.

DÜLGER, Murat Volkan, **Ceza Hukuku Genel Hükümler**, Seçkin Yayıncılık, 2. Baskı, 2023.

ERDAĞ, Ali İhsan, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C. 14, Sa: 2, Y. 2010.

ERDOĞAN, Yavuz, **Türk Ceza Kanunu'nda Bilişim Suçları**, Legal Yayıncılık, İstanbul, 2012.

EREN, Ahu Karakurt, "Bilişim Alanında Suçların veya Bilişim Sistemlerinin Araç Olarak Kullanıldığı Diğer Suçların İşlenmesi Amacıyla Cihaz, Program, Şifre ya da Güvenlik Kodlarının Üretilmesi, Yayılması veya Bulundurulması Suçu", **Türkiye Adalet Akademisi Dergisi**, Sa: 43, Y. 2020.

ERMEYDAN, Damla, **Türk Ceza Kanununda Bilişim Suçları**, Güncellenmiş 2. Baskı, Seçkin Yayıncılık, Ankara, 2023.

GÜL, Ahmet, **Doğrudan-Dolaylı Bilişim Suçları**, Genişletilmiş, Güncellenmiş ve Yenilenmiş 3. Baskı, Seçkin Yayıncılık, Ankara, 2021.

İÇEL, Kayıhan, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", **İstanbul Hukuk Mecmuası**, C. 59, Sa: 1-2, Y. 2011.

İÇER, Zafer, **Suça Teşebbüste Hazırlık Hareketleri ile İcra Hareketlerinin Birbirinden Ayrılması**, On İki Levha Yayıncılık, Haziran 2021.

KARADENİZ, Yusuf, "Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ve Türk Hukuku'nda Karşılığı", **Güvenlik Bilimleri Dergisi**, C. 11, Sa: 1, Y. 2022.

KARAGÜLMEZ, Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Genişletilmiş ve Gözden Geçirilmiş 3. Baskı, Seçkin Yayıncılık, Ankara, 2011.

KAYA, İslam Safa/ÇAKIR, Adem, "Yasak Cihaz veya Programlar Suçu", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, C. 19, Sa: 38, Y. 2020.

KAZAKER BOZKURT, Gözde "Cezalandırılabilirliğin Öne Çekilmesi - Kavram, Nedenleri, Görünüm Şekilleri (Alman Ceza Hukuku ile Karşılaştırmalı Bir İnceleme)", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C: 24, S: 1, 2022, s. 241 - 288.

KEÇELİOĞLU Elvan Keçelioğlu, "Sırf Hareket Suçu Soyut Tehlike Suçu Mudur?", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi,** C. 25, Sa. 2, Yıl: 2021.

KERMAN, Onur Kemal, Hazırlık Hareketlerinin Cezalandırılması, **Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yayımlanmamış Doktora Tezi**, Mart 2024.

KOCA, Mahmut/ÜZÜLMEZ, İlhan, **Türk Ceza Hukuku Genel Hükümler**, 16. Baskı, Adalet Yayınevi, Ankara 2023.

KOCA, Mahmut/ÜZÜLMEZ, İlhan, **Türk Ceza Hukuku Özel Hükümler**, 6. Baskı, Adalet Yayınevi, Ankara 2019.

MERAN, Necati, **Sahtecilik - Malvarlığı Bilişim Suçları ile Ekonomik ve Ticaret Alanında Suçlar**, Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Seçkin Yayıncılık, Ankara, 2008.

ÖNOK, Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 19, No: 2, 2013.

ÖZBEK, Veli Özer/DOĞAN Koray, BACAKSIZ Pınar, **Türk Ceza Hukuku Özel Hükümler**, Genişletilmiş ve Güncellenmiş 18. Baskı, Eylül 2023, Seçkin Yayıncılık, Ankara, 2023.

ÖZBEK, Veli Özer/ DOĞAN, Koray/ Serkan MERAKLI/ Pınar BACAKSIZ/ İsa BAŞBÜYÜK, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayıncılık, 15. Baskı, 2024.

ÖZGÜÇ, Levent Emre, 5846 Sayılı Fikir ve Sanat Eserleri Kanunu m.72'de Yer Alan "Teknolojik Önlemleri Etkisiz Kılma" Suçunun Değerlendirilmesi, Suç Genel Teorisi ve Ceza Adaleti Bağlamında Güncel Mevzuat Değişikliklerine İlişkin Değerlendirmeler, **İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Ceza Hukuku Sempozyumu Tam Metin Bildirileri Kitabı**, Nisan 2024.

ÖZGÜÇ, Levent Emre, Türk Ceza Hukukunda Hazırlık Hareketlerinin Belirlenmesi ve Cezalandırılabilirliği, Oniki Levha Yayıncılık, Ağustos 2024.

SARITAŞ, Erkan, "Cezalandırılmayan Önceki Hareketler", **İstanbul Hukuk Mecmuası**, C. 80, Sa. 2.

SİEBER, Ulrich Vd., **Bilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku**, Birinci Baskı: Mayıs 2021., Seçkin, Ankara, 2021.

TAŞKIN, Şaban Cankat, Ceza Hukukunda Cezalandırılabilirliğin Ön Alana Kaydırılması ve Hazırlık Hareketlerinin Cezalandırılması Sorununun Yasak Cihaz veya Programlar Suçu Özelinde İngiliz Ceza Hukuku, Kanada Ceza Hukuku ve Avrupa Konseyi Siber Suç Sözleşmesindeki Düzenlemelerle, **Ceza Hukuku Dergisi**, C. 19, Sa. 55, Y. 2024.

TEKİN, Derya, "Bir Ceza Politikası Olarak Hazırlık Hareketlerinin Cezalandırılması: Türk ve İngiliz Yasal Düzenlemelerinin Karşılaştırmalı Analizi", **Terazi Hukuk Dergisi**, C. 13, Sa: 147, Y. 2018.

TEZCAN, Durmuş/Erdem, Mustafa Ruhan/ÖNOK, R. Murat, **Teorik ve Pratik Ceza Özel Hukuku**, Güncellenmiş 21. Baskı, Eylül 2023, Seçkin Yayıncılık, Ankara, 2023.

TUNÇER, Asuman İnce, "Yasak Cihaz ve Programlar Suçu (TCK m.245/A)", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C. 32, Sa: 3, Y. 2024.

ÜNAL, Osman Gazi, "Cezalandırılabilirliğin Ön Alana Kaydırılması Bağlamında, Yasak Cihaz veya Programlar Suçu (TCK m.245/A)", **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C. 26, Sa: 2, Y. 2022.

YENİDÜNYA, A. Caner/DEĞİRMENCİ, Olgun, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, Legal Yayıncılık, İstanbul, 2003.

YETKİN, Erdi, **Cezalandırılabilirliğin Öne Alınmasının Bir Görünüş Biçimi Olarak Hazırlık Hareketlerinden Doğan Ceza Sorumluluğu**, İstanbul Arşivi, Oniki Levha Yayıncılık, Şubat 2024.