CEZALANDIRILABİLİRLİĞİN ÖN ALANA KAYDIRILMASI BAĞLAMINDA, YASAK CİHAZ VEYA PROGRAMLAR SUÇU (TCK M. 245/A)

Osman Gazi ÜNAL[*]

ÖZET

Teknolojinin gelişmesiyle birlikte bilişim alanında işlenen suçlarla mücadele etmek, artık daha karmaşık bir hale gelmiştir. Bu suçların sınıraşan boyutunun olması devletleri, uluslararası alanda bir işbirliğine götürmüştür. Bu işbirliğinin bir sonucu olarak Avrupa Konseyi Siber Suç Sözleşmesi akdedilmiştir. Sözleşmenin 6. maddesiyle taraf devletler, bilişim alanındaki suçların işlenmesine yönelen cihaz, şifre, erişim kodu veya benzeri bir veri oluşturmayı ve imal etmeyi suç haline getirmekle yükümlü kılınmışlardır. Bu doğrultuda hem bu suçları önleyebilmek hem de bu suçların işlenmesine kaynaklık eden karaborsanın oluşumunu engellemek amacıyla ceza hukuku müdahalesinin hazırlık hareketlerine doğru kaydırılması öngörülmüştür. Sözleşmedeki bu yükümlülüğe uygun olarak TCK 245/A maddesiyle "yasak cihaz veya programlar" suçu ihdas edilmiştir. Bu suç kapsamında bilişim alanındaki suçlar ve bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların hazırlık hareketleri cezalandırılmıştır. Bu çalışmada öncelikle hazırlık hareketlerinin cezalandırılmasına dair meşruiyet kriterleri ele alınmıştır. Akabinde TCK m. 245/A hükmü, Alman Ceza Kanunu'da yer alan ilgili suç tipleriyle karşılaştırılmalı olarak incelenmiştir. Son olarak inceleme sonucunda ortaya çıkan birtakım sorunlara da çözüm getirilmeye çalışılmıştır.

Anahtar Kelimeler: *Hazırlık hareketleri, Avrupa Konseyi Siber Suç Sözleşmesi, bilişim alanında suçlar, yasak cihaz veya programlar, şifre veya sair güvenlik kodu.*

OFFENCE OF PROHIBITED DEVICES OR COMPUTER PROGRAMS (TPC, SECTION 245/A), IN THE CONTEXT OF PREPONING CRIMINAL LIABILITY

ABSTRACT

With the advancement of technology, it has now become more complex to fight against the offences related to data processing systems. The transnational aspect of these offences has led the states to a collaboration. As a result of this collaboration,

---

[*] **Dr. Arş. Gör,** Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Anabilim Dalı/ANKARA, **e-posta:** osman.unal@hbv.edu.tr,
ORCID: 0000-0002-3101-0645.
DOI : 10.34246/ahbvuhfd.1116684

Yayın Kuruluna Ulaştığı Tarih : 12/08/2021

Yayınlanmasının Uygun Görüldüğü Tarih: 02/01/2022

The Council of European Convention on Cybercrime was signed. By the article 6 of the Convention, contracting states are obliged to criminalize the composing and manufacturing of a device, computer password, access code or similar data directed committing offence in the field of data processing systems. Accordingly, it is envisaged that criminal law should be preponed towards prepatory acts in order both to prevent the commitment of these offences and to block the formation of the black market which is the source of these offences. In accordance with this obligation in the Convention, the offence of "prohibited devices or computer programs" was set forth in the article 245/A of the Turkish Penal Code (TPC). Within the context of this crime, the prepartory acts of offences related to data processing systems and other offences that may be committed by using an instrument data processing system are punished. In this study, firstly, the legitimacy criteria for the punishment of prepatory acts have been considered. Afterwards, the article 245/A of the TPC has been examined comparatively with the relevant offences in the German Penal Code. Finally, some problems we detected as a result of our examination have also tried to be solved.

Keywords: *Preparatory acts, the Council of European Convention on Cybercrime, offenses related to data processing systems, prohibited devices or computer programs, password or other security code.*

GİRİŞ

Hazırlık hareketleri kural olarak cezalandırılmasa da hukuk düzeni, hukuki değerleri daha etkin bir şekilde koruyabilmek amacıyla ceza hukuku müdahalesini, önalana doğru çekmektedir. Bu yöntemle bir hazırlık hareketi ayrı bir suç tipi haline getirilmekte ve ileride gerçekleşebilecek zararların önlenmesine çalışılmaktadır. Dolayısıyla ceza hukuku "baskıcı-sınırlayıcı"dan, "önleyici-şekillendirici" bir modele doğru dönüşüm geçirmektedir. Fakat bu durum aynı zamanda temel hak ve özgürlüklerin geniş bir şekilde sınırlandırılması sonucunu doğurmaktadır. Bu yüzden dengenin sağlanması adına yeni suç tiplerinin, ceza hukukunun klasik alanından tamamen farklı bir şekilde ihdas edilmemesi gerekir. Aksi takdirde bu suç tiplerinin maddi açıdan meşruiyeti tartışmaya açık olacaktır.

Bilişim alanında görülen gelişmeler, bu alanda işlenen veya bilişim suretiyle işlenen diğer suçların artmasına da ön ayak olmuştur. Bu suçların işlenmesinin kolaylaşmasıyla bireylerin yanı sıra, ilgili ülkenin güvenliği de tehlike altına girmektedir. Bu bağlamda bilişim alanında işlenen suçlarla mücadelenin daha etkin bir şekilde yürütülmesi gerekliliği ortaya çıkmıştır. Diğer alanlarda olduğu gibi bilişim alanında işlenen suçlar bakımından da cezalandırılabilirliğin ön alana kaydırılması (Vorverlagerung) konusunun

incelenmesine ihtiyaç vardır. Nitekim bu suçların hazırlık hareketlerinin ayrı bir suç tipi olarak cezalandırılması gerektiği yönünde hem milli düzeyde hem de milletlerarası alanda bir irade oluşmuştur. Bu bakımdan hem bilişim alanında oluşan suçlarla etkin mücadele yürütebilmek hem de bu alanda uluslararası işbirliğini sağlamak amacıyla Avrupa Konseyi Siber Suç Sözleşmesi oluşturulmuştur.

Konuyla ilgili olarak öncelikle bilişim alanında veya bilişim sistemlerinin araç olarak kullanılmasıyla işlenen suçlarda cezalandırılabilirliğin ön alana kaydırılması konusu incelenmelidir. Akabinde AK-SSS'nin ilgili hükümleri, TCK'nın 245/A hükmünde düzenlenen yasak cihaz veya programları suç tipi, Alman Ceza Kanunu'ndaki (StGB) ilgili suç tipleriyle birlikte karşılaştırmalı bir şekilde ele alınacaktır. Ayrıca bu suçla ilgili olarak uygulamaya yansıyacak çeşitli sorunlardan da bahsedilerek çözüm önerileri sunulacaktır.

I. BİLİŞİM ALANI VE BİLİŞİM SİSTEMLERİNİN ARAÇ OLARAK KULLANILMASI SURETİYLE İŞLENEN SUÇLARDA CEZALANDIRILABİLİRLİĞİN ÖN ALANA KAYDIRILMASI SORUNU

A. Cezalandırılabilirliğin Ön Alana Kaydırılması

Suç yolunda (iter criminis) icra hareketleri henüz başlamadığı için hazırlık hareketleri kural olarak cezaya tabi değildir. Nitekim suça teşebbüse ilişkin TCK m. 35 hükmündeki "*doğrudan doğruya icraya başlayıp*" ibaresi bu hususa vurgu yapmaktadır. Bununla birlikte hazırlık hareketleri failin suç planına göre bile suçun tamamlanmasından o kadar uzaktır ki, herhangi bir hukuki değer ihlalinden bahsedilemez[1]. Diğer bir ifadeyle bu hareketler, neticeye çok uzak olduklarından hukuki değer ihlaline yol açan ciddi bir tehdit oluşturmamaktadırlar. İcra hareketleri ise hazırlık hareketine nazaran bir müdahale karakterini (Angriffscharackter) haizdir[2]. İlaveten hazırlık hareketlerinin bir suça yöneldiği olgusu genel itibariyle şüphe içerisinde kalmaktadır ve bunun ispatının zor olduğu ifade edilmektedir[3]. Keza teşebbüste kastın belirlenme sorunu ya da failin suç işlemeye yönelik

[1] Ulrich Weber, "Die Vorverlagerung des Strafrechtschutzes durch Gefährdungs und Unternehmensdelikte", *Beiheft zur Zeitschrift für die gesamte Strafrechtwissenschaft*, Walter de Gruyter, 1987, s. 15.

[2] Willy Pütz, "Der Gefahrbegriff im Strafrecht", Universität Köln, *Dissertation,* 1936, s. 21.

[3] Mehmet Emin Artuk / Ahmet Gökcen / Kerim Çakır / Zafer İçer, *Türk Ceza Hukuku: Genel Hükümler, 14. Baskı*, Adalet Yayınevi, 2020, s. 683.

kararından vazgeçme ihtimalinin yüksek olması da hazırlık hareketlerinin cezalandırılmamasına gerekçe sunar[4].

Esasında hazırlık hareketlerinin cezalandırılması kanunilik ilkesiyle bağdaşmamaktadır. Daha ziyade bu hareketler, hukuki değeri ihlal eden icrai hareketlerin hazırlanmasına hizmet ederler[5]. Ancak kanun koyucu, cezasız olmalarına rağmen, hazırlık hareketlerine ceza tehdidini öngörerek bu alanı müstakil suç olarak düzenleme yoluna başvurmaktadır[6]. İzlenen bu yöntem kanunilik ilkesiyle uyumludur. Nitekim bazı hukuki değerler o kadar önemlidir ki bununla ilişkili olan suçun konusu üzerinde bir zarar veya bir tehlikenin oluşması istenmemektedir. Hazırlık hareketlerinin dar anlamda bizzat bir hukuki değeri ihlal etmediğine, ancak gelecekte kasıtlı bir şekilde ihlal edileceği ihtimalinin gündeme geldiğine ve bu yüzden cezalandırılabilirlik yolunun açıldığına değinilmektedir[7]. Bu noktada bazı bireyüstü (veya kamusal) hukuki değerlerin var olduğu belirtilerek bunlar aracılığıyla zarar oluşturulan hareket ötelenerek bireysel hukuki değerlerin önalanda korunması amaçlanabilir[8]. Bu durum cezalandırılabilirliğin önalana kaydırılması düşüncesini akla getirmektedir. Böylelikle kanun koyucu, suçun konusu üzerinde bir zarar veya bir tehlike oluşturmayan hareketleri dahi bir hukuki değer ihlali olarak kabul etmektedir. Kanaatimizce de hazırlık hareketleri müstakil bir suç olarak düzenlendiği takdirde suçun işlenmesiyle birlikte artık hukuki değer ihlalinin oluşmadığından bahsedilemez.

Cezalandırılabilirliğin ön alana kaydırılması aynı zamanda önleyici

---

4 Berrin Akbulut, *Türk Ceza Hukuku: Genel Hükümler*, 4. Bası, Adalet Yayınevi, 2017, s. 565; Örneğin, bir akaryakıt istasyonundan birkaç litre benzin satın alan kişinin yangın çıkarma (TCK m. 170) ya da mala zarar verme suçu (TCK m. 151) bağlamında bir hazırlık hareketi olduğu belirtilebilir. Fakat her benzin satın alan kişinin bu suçları işlemek amacında olduğu söylenemez. Zira yolda kalan aracı çalıştırmak gayesiyle de benzin satın alınabilir. Bkz. Artuk / Gökcen / Çakır / İçer, s. 684.

5 Pütz, s. 21.

6 Pütz, s. 24; Aynı yönde bkz. Akbulut, *Genel Hükümler*, s. 566.

7 Jens Puschke, "Grund und Grenzen des Gefährdungsstrafrechts am Beispiel der Vorbereitungsdelikte", Roland Hefendehl (Ed.), *Grenzenlose Vorverlagerung des Strafrechts?,* Berliner Wissenschafts Verlag, 2010, s. 11.

8 Ulrich Sieber, *Bilişim Teknolojisi İle Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku*, Feridun Yenisey / Salih Oktar / Zehra Başer Doğan (Çev.), Seçkin Yayıncılık, 2021, s. 438; Kanaatimizce tüm hukuki değerler bireye aittirler ve birey temelli olarak yorumlanmalıdırlar. İlgili açıklamalar için bkz. Osman Gazi Ünal, Türk Ceza Hukukunda Tehlike Suçları, *Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Yayımlanmamış Doktora Tezi*, 2020, s. 116 vd.

ceza hukuku anlayışını gündeme getirmektedir. Önleyici ceza hukuku anlayışı ile çokça tartışılan risk ceza hukuku anlayışı arasında hemen hemen bir fark bulunmamaktadır. Suç öncesinin cezalandırılmasıyla amaçlanan husus, gelecekte gerçekleşebilecek suçların işlenmesinin önüne geçmektir[9]. Nitekim bir başka suça hazırlık kapsamında olan kasıtlı veya bazı hallerde taksirli fiiller dahi bizatihi suç sayılarak ağır neticeler doğurabilecek suçların işlenmesinden çok önceye yönelik bir önleme iradesi oluşmuştur. Dolayısıyla cezalandırılabilirlik alanı, önlenmesi amaçlanan nihai zarardan o kadar uzak bir noktaya kadar genişlemiştir ki geleneksel (çekirdek) ceza hukuku alanının dışına çıkılmış olur[10].

Cezalandırılabilirliğin ön alana kaydırılmasının çeşitli görünüm şekilleri bulunmaktadır. Teşebbüs suçlarının, diğer bir isimle kalkışma suçlarının oluşturulması bunun bir yönüdür. Diğer yön ise yukarıda da bahsi geçtiği üzere, icra hareketlerinin de ötesine kaydırılması suretiyle hazırlık hareketlerinin cezalandırılmasıdır[11]. Bu diğer yön aynı zamanda bazı meşruiyet sorunlarını ortaya çıkarmaktadır. Zira hazırlık hareketlerinin cezalandırılmasının; kusur sorumluluğu, son çare olma, ceza sorumluluğunun şahsiliği ve orantılılık gibi temel ceza hukuku ilkeleriyle bağdaşması oldukça güçtür.

Bu meşruiyet sorununun aşılabilmesi için birtakım önerilerde bulunulmuştur. Buna göre, hareketin ancak nesnel olarak zarar verme eğilimini içermesi durumunda suç kapsamına alınmasının meşru olduğu ifade edilmelidir. Keza zararlı neticenin önlenmesi bağlamında bir zorunluluk varsa tehlikenin oluşmasını suç kapsamına almak meşru görülmektedir[12]. İlgili öneriler doğrultusunda bunun sınırları da çizilmektedir. İlk olarak hazırlık hareketlerini cezalandırılan suçların, hukuki değere aşırı derecede müdahalede bulunmaması gerektiği ileri sürülmektedir[13]. Aynı zamanda failin cezalandırılabilir davranışı ile korunan hukuki değer arasında özel bir ilişki bulunmalıdır[14]. İlaveten hangi hazırlık hareketinin hangi hukuki değere

[9] Fakat bu durumun da yanıltıcı olduğu belirtilerek ihdas edilen her bir suçun önleme amacının bulunduğuna vurgu yapılmıştır. Bkz. Ali Emrah Bozbayındır, "The Advent of Preventive Criminal Law: An Erosion of The Traditional Criminal Law?" *Criminal Law Forum,* (29), 2018, s. 26.

[10] Bozbayındır, s. 27.

[11] Weber, s. 15.

[12] Weber, s. 15, 16.

[13] Puschke, s. 24.

[14] Sieber, s. 438.

yöneldiği belirli olmalıdır. Yalnızca tehlikeli, yani belirli bir zarar verme eğilimi olan tipik hazırlık hareketlerinin cezalandırılması orantılılık ilkesine uygun olur. Son olarak buna ilişkin normlar somut olmalı ve belirlilik ilkesine uygun şekilde ihdas edilmelidir[15].

Hazırlık hareketlerini suç haline getiren hükümlerin meşruiyeti ile ilgili doktrinde yapılan tartışmalar, 2009 yılında düzenlenen 18. Uluslararası Ceza Hukuku Kongresi'ne de yansımıştır. Böylelikle genel cezalandırma politikası aşılarak hazırlık hareketlerinin suç olarak ihdas edilebilmesi için, ulusal standartların yanında uluslararası standartlar da öngörülmüş olmaktadır[16]. Kongre'de konuya ilişkin şu sonuçlara ulaşılmıştır:

> *"1. Çok önemli hukuki değerlere zarar verecek çok ciddi bir saldırının önlenmesi;*
>
> *2. Hukukun hangi hazırlık hareketlerinin cezalandırılacağını çok genel ifadelere başvurmaktan kaçınarak tanımlamış olması;*
>
> *3. Suç haline getirilen fiillerin asıl suçun işlenmesine sıkı sıkıya bağlı olması;*
>
> *4. Cezanın, işlenmiş suç için öngörülenden daha hafif olması ve de aynı kişi tarafından işlenmiş ana suç için öngörülmüş ceza ile birleştirilerek veya hafifletilerek ilgili teşebbüs yaptırımına uygun hale getirilmesi."*[17]

Ulaşılan bu sonuçlar hazırlık hareketlerinin cezalandırılmasında adeta birer kriter olarak ele alınabilir. Cezalandırılabilirliğin ön alana kaydırılması noktasında bahsi geçen önerilere ve bu kriterlere riayet edilmeksizin yapılan kanuni düzenlemeler, meşruiyet kriziyle karşılaşabileceği gibi temel hak ve özgürlükleri de aşırı bir şekilde kısıtlayacaktır.

Geçmişte cezai sorumluluğunun ön alana kaydırılması, devlet güvenliği, yol güvenliği ve toplum için tehlikeli olan bireysel eylemlerle ilgiliydi. Bugün ise çevre, ekonomi alanlarında teknolojinin kullanımıyla birlikte örgütlü suç ve uluslararası terörizmle ilgilidir. Buna bilişim veya siber alan da dahildir.

---

[15] Puschke, s. 24.

[16] Derya Tekin, "Bir Ceza Politikası Olarak Hazırlık Hareketlerinin Cezalandırılması: Türk ve İngiliz Yasal Düzenlemelerin Karşılaştırmalı Analizi", *Terazi Hukuk Dergisi,* 13(147), 2018, s. 49.

[17] Bkz. Türk Ceza Hukuku Derneği, 18. Uluslararası Ceza Hukuku Kongresi, Hazırlık Hareketleri ve İştirakin Genişlemesi, <https://www.tchd.org.tr/18-uluslararasi-ceza-hukuku-kongresi/#1541890191101-bb047707-5831>, Erişim Tarihi 27 Eylül 2021.

Bu alanlarda karşılaşılan tehlikeler, bunların boyutunu düşürmeyi ifade eden kanuni tiplerin meşrulaştırılmasının başını çekmektedir[18].

Bilişim alanında gelişmeler, bireyin hayatını kolaylaştırdığı gibi onun yeni suç tipleriyle yüzleşmesine neden olmuştur. Benzer şekilde devletler de sistemlerini bilişim alanına dahil etmekle birlikte bu alanda gerçekleşen saldırılara karşı açık hale gelmiştir[19]. Zira modern bilişim sistemleri karmaşık yapılı olsalar da kullanıcıların kolay bir şekilde yararlanmaları istendiğinden saldırılara karşı savunulmaları zordur[20]. Bu saldırılara açık hale gelme hali sadece vatandaşların verilerinin çalınmasıyla ve bilişim suretiyle işlenen dolandırıcılık ya da hırsızlık suçlarıyla sınırlı değildir. Saldırı sonucunda devletin vatandaşlarına vermiş olduğu hizmet de aksayabilmektedir. Örneğin, Estonya'ya yapılan siber saldırı sonucunda acil durum aramaları bir saate kadar işlevsiz hale getirilmiştir. Keza bu saldırı bizzat devletin güvenliğine karşı savaş zamanında da yapılabilmektedir. 2008 yılının Ağustos ayında yaşanan Rusya'nın Güney Osetya'yı işgali sırasında, Gürcistan'ın internet bağlantısı kesilerek dünya ile bağlantısına son verilmiştir[21]. Bu nedenle hem bireylerin bilişim sistemlerine olan güvenirliliğini ihlal edebilecek riskleri en aza indirmek hem de devletlerin bilişim alanındaki güvenliğine zarar verebilecek girişimleri önleyebilmek adına düzenleme yapma ihtiyacı hasıl olmuştur. İlgili bu düzenlemeler ihdas edilirken klasik ceza hukuku araçları da dahil olmak üzere devletlerin aldığı tedbirlerin yetersiz kaldığına, bilişim alanındaki gelişmelerin sınıraşan bir boyutunun[22] olduğuna ve bu yüzden uluslararası bir mücadeleyi gerektirdiğine işaret edilmiştir[23]. Her ne kadar devletlerin aldığı

---

18 Puschke, s. 10.

19 Merve Erdem / Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 69(1), 2019, s. 129.

20 Sieber, s. 260.

21 Erdem / Gözocak, s. 130.

22 Örneğin, bilişim suçlarında fail belirli bir devletin yargı yetkisi içerisinde iken işlemiş olduğu fiiller ile başka ülkelerdeki bilişim sistemlerine müdahale edebilmekte ve birçok kişinin mağdur olmasına yol açabilmektedir. Bkz. Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Prof. Dr. Nur Centel'e Armağan*, 19(2), 2013, s. 1234.

23 Ahu Karakurt Eren, "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,* 11(43), 2020, s. 221.

önlemler ve ihdas ettiği hukuki düzenlemeler kapsamlı veya etkin görünse de bilişim suçlarının doğası gereği genellikle etkili olamamaktadırlar[24].

Bu uluslararası mücadele, bilişim alanında hazırlık hareketlerinin cezalandırılmasını öngörmektedir. İlaveten bu ön alanı cezalandıran kanuni tipler belirli risklerle mücadelede kullanılmaktadır ve Avrupa Birliği bünyesindeki çeşitli kurumlar tarafından da teşvik edilmektedir[25]. Gelecekte, hazırlık hareketlerinin cezalandırılması veya hazırlık ceza hukuku (Vorbereitungsstrafrechts) alanında, Avrupa Birliği hukukuna ilişkin direktiflerin, daha da yoğunlaşması beklenmektedir[26]. Bu doğrultuda yeni suç tiplerinin ihdası gündeme gelmektedir. Ayrıca bu durum cezaya liyakat ve muhtaçlık ya da meşruiyet sınırlarının nereye kadar çizileceği sorunlarını da beraberinde getirmektedir.

B. Avrupa Siber Suç Sözleşmesindeki Durum

Bilişim alanında cezalandırılabilirliğin hazırlık hareketlerine doğru genişlemesinin itici gücü her şeyden evvel devletlerarasındaki **i**şbirliği arzusudur[27]. Bu işbirliği arzusu zarar oluşturan suçların zarar veya tehlike oluşmadan da önlenebileceği düşüncesine dayanmaktadır. Bu doğrultuda Avrupa Suç Sorunları Komitesi'nin CDPC/103/211196 sayılı kararıyla bilişim suçlarıyla (siber suçlarla) ilgilenecek bir uzmanlar komitesi kurulmuştur[28]. Oluşturulan komitenin başlıca amacı, bu suçlarla ilgili belli alanları inceleyerek bağlayıcı bir hukuki metin ortaya koymaktır[29]. Komitenin çalışmaları sonucunda Avrupa Konseyi Siber Suç Sözleşmesi ve sözleşmenin adeta gerekçesini oluşturan açıklayıcı memorandumu (açıklayıcı rapor) hazırlanmıştır. Dolayısıyla sözleşme bilişim alanında en kapsamlı uluslararası düzenleme olma özelliğini haizdir[30].

Sözleşme 23.11.2001 tarihinde Budapeşte'de imzaya açılmıştır.

---

[24] Cahit Aliusta / Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci, *Uluslararası Bilgi Güvenliği Dergisi*, 4(2), 2018, s. 36.

[25] Puschke, s. 11.

[26] Puschke, s. 19.

[27] Puschke, s. 17.

[28] Avrupa Konseyi Siber Suç Sözleşmesi Açıklayıcı Memorandum, 2.7 paragraf, <https://rm.coe.int/16800cce5b#:~:text=The%20Convention%20and%20its%20Explanatory,II>, Erişim Tarihi 05 Ekim 2021.

[29] Önok, s. 1241.

[30] Sieber, s. 268.

Sözleşmeyi sadece Avrupa Konseyi'ne üye olan devletler değil, Kanada, Japonya, Arjantin, İsrail ve ABD de imzalamışlardır[31]. Türkiye sözleşmeye 10.11.2010 tarihinde imza koymuştur[32]. Sözleşme, "Sanal Ortamda İşlenen Suçlar Sözleşmesi" adıyla 22.04.2014 tarihli 6533 sayılı Kanunla onaylanması uygun bulunmuş olup 02.05.2014 tarihinde yürürlüğe girmiştir[33].

Sözleşmenin açıklayıcı memorandumunun 3. başlık 15 no.lu paragrafında sözleşmenin amaçlarından bahsedilmiştir. Bu amaçlar:

> "(*1) siber suçlar alanında maddi ceza hukuku unsurlarını ve bağlantılı hükümleri uyumlu hale getirmek*[34]*,*
>
> *(2) bu suçların ve bir bilgisayar sistemi kullanılarak işlenen ya da delilleri elektronik formda olan başka suçların soruşturulması ve kovuşturulması için gerekli olan yerel ceza usulleri hukuku yetkilerini sağlamak*
>
> *(3) hızlı ve etkin bir uluslararası işbirliği rejimi oluşturmak*"

şeklinde öngörülmüştür. Ayrıca sözleşmenin dört bölümden oluştuğu görülmektedir. İlk bölümde suç tanımları, ikinci bölümde bilişim suçlarıyla mücadelede alınacak ulusal düzeydeki önlemler, üçüncü bölüm uluslararası adli yardımlaşmayla ilgili düzenlemeler, dördüncü bölümde ise diğer hükümler yer almaktadır. Sözleşmedeki hükümler ve sözleşmenin açıklayıcı memorandumu taraf ülkelerin ihdas ettiği düzenlemelerin yorumlanması amacıyla da kullanılmaktadır[35].

---

[31] Sözleşmeye imza koyan ve onaylayan ülkeler listesi için bkz. Chart of signatures and ratifications of Treaty 185, Title: Convention on Cybercrime, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>, Erişim Tarihi 05 Ekim 2021.

[32] Sözleşmeye imza konulmuşsa da hemen iç hukuka aktarılamamıştır. Zira adli yardım taleplerine sözleşmenin öngördüğü biçimde ve hızlı olarak karşılık vermeye mümkün hale getirecek altyapı ihtiyacının ülke çapında mevcut olmaması buna gerekçe oluşturmaktaydı. Bkz. Önok, s. 1242.

[33] 6533 sayılı Kanun, RG: 28988, <https://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm>, Erişim Tarihi 06 Ekim 2021; Sözleşme bakımından ileri sürülen çekinceler ve beyanlar için bkz. 09.08.2014 tarihli, 2014/6656 sayılı Karar, <https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5.htm>, Erişim Tarihi 06.10.2021.

[34] Bilişim suçlarının karşılaştırmalı hukukta yeknesak bir tanımı bulunmadığına, var olan tanımların da belirli ve yeterli içerikte olmadığına değinilmektedir. Bkz. Aliusta / Benzer, s. 36; Nitekim, bu yeknesaklığın sağlanmaması etkili bir adli yardımlaşmanın yürütülmesine de engel teşkil eder. Bkz. Önok, s. 1233.

[35] Jörg Eisele, "Der Kernbereich des Computerstrafrechts", *JURA,* Heft 12, 2021, s. 923.

Sözleşmenin ilk bölümünde "**Cihazların Kötüye Kullanımı**" başlıklı 6. maddesiyle sözleşmedeki bilişim suçlarıyla ilgili olarak hazırlık hareketlerinin cezalandırılması öngörülmüştür[36]. 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[37]. İlaveten devletler oluşturulan bu verilerin veya imal edilen ürünlerin satışını, kullanmak maksadıyla temin edilmesini, bulundurulmasını, ithalini, dağıtımını veya başka bir şekilde erişilebilir hale getirilmesini de ceza tehdidiyle karşılamak yükümlülüğü altındadırlar.

Sözleşme, cezalandırılabilirliğin ön alana kaydırılması suretiyle bilişim suçlarının işlenmesinin önüne geçmeyi amaçlamaktadır. Bunun yanında madde hükmüyle ulaşılmak istenen asıl hedef, uluslararası alanda bilgisayar korsanlığı (hacker) olgusuyla mücadele edebilmek ve bu amaca yönelik tahsis edilen

---

[36] Sözleşmenin 6. maddesi aynen şu şekildedir:

"*1. "Taraflardan her biri, kasten ve haksız yere gerçekleştirildiği zaman, aşağıdakilerin kendi iç hukuku kapsamında cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:*

a. Aşağıda belirtilenlerin 2 ila 5. maddelerde belirtilmiş herhangi bir suçun işlenmesi için kullanılmaları amacıyla üretimi, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı veya başka şekilde erişilebilir hale getirilmesi:

i. bir bilgisayar programı da dâhil olmak üzere, öncelikli olarak yukarıda belirtilen 2 ila 5. maddelerde belirtilmiş herhangi bir suçu işlemek amacıyla tasarlanmış veya uyarlanmış bir cihaz;

ii. bir bilgisayar sisteminin tamamına veya herhangi bir kısmına erişimi mümkün kılan bir bilgisayar şifresi, erişim kodu veya benzer bir veri.

ve

b. Yukarıda paragraf a.i veya ii' de atıfta bulunulmuş bir öğeye, 2 ila 5. Maddelerde belirtilmiş herhangi bir suçun işlenmesi için kullanılması amacıyla bulundurma. Taraflardan biri, yasa gereği cezaî sorumluluğun doğması için bahsi geçen öğelerden belli bir sayıda bulundurulmasını şart koşabilir.

2. İşbu madde, bu maddenin 1. paragrafında atıfta bulunulan üretme, satma, kullanım amaçlı tedarik, ithalat, dağıtma veya başka şekilde erişilebilir hale getirme veya bulundurmanın, 2 ila 5. maddeler uyarınca suç işlemek maksadıyla gerçekleştirilmemesi durumunda, örneğin bir bilgisayar sisteminin yetkililerce test edilmesi veya korunmasının amaçlandığı hallerde, cezaî yükümlülük doğuracağı şeklinde yorumlanmayacaktır.

3. Taraflardan her biri, çekincenin işbu maddenin l..a.ii paragrafında sözü edilen öğelerin satışı, dağıtımı veya başka şekilde erişilebilir hale getirilmesiyle alakalı olmaması kaydıyla, işbu maddenin 1. paragrafını uygulamama hakkını saklı tutabilir."

[37] İslam Safa Kaya / Adem Çakır, "Yasak Cihaz veya Programlar Suçu", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, (38), 2020, s. 36.

araçların karaborsasının oluşmasını engellemektir[38]. Bu karaborsanın oluşumu, aynı zamanda "siber terörizm"in yaygınlaşmasına da zemin hazırlamaktadır. Zira bu amaçla hareket eden gruplar; gerekli teknik ekipmanı, yöntem bilgisi, veri tabanlarını ve programları bu karaborsadan bulabilmektedir[39]. Böyle bir karaborsanın oluşumu aynı zamanda başka suçların işlenmesine de zemin hazırlamaktadır. Örneğin, bu amaçla üretilen bir cihazı temin etmek isteyen bir kimse dolandırıcılık suçuna maruz kalabilmektedir. Keza bu amaca yönelik karaborsadan elde edilen şifre dolayısıyla kişinin verileri de çalınabilmekte veya kaybolabilmektedir.

II. YASAK CİHAZ VE PROGRAMLAR SUÇU (TCK M. 245/A)

A. Suç Tipiyle İlgili Genel Bilgiler

Hazırlık hareketlerinin cezalandırılmaması esas kabul edilse de TCK'da bazı suçlarla ilgili olarak bunların cezalandırılması için birtakım özel hükümler ihdas edilmiştir. Diğer bir anlatımla hazırlık hareketlerinin cezalandırılması, bazı suç tipleriyle sınırlı olmak kaydıyla TCK'nın sistemine bütünüyle yabancı değildir. Bunun en bilinen örneğini TCK m. 220 hükmündeki **suç işlemek amacıyla örgüt kurma** suçu oluşturur. Keza TCK m. 200 hükmünde düzenlenen **parada ve kıymetli damgaları yapmayı yarayan araçlar** suçuyla bu alanda işlenen suçların önlenmesi amaçlanmıştır. Yine TCK m. 174 hükmünde yer alan **tehlikeli maddelerin izinsiz olarak bulundurulması veya el değiştirilmesi** suçuyla hayata, vücut dokunulmazlığına, toplum veya çevreye karşı işlenecek suçların hazırlık hareketleri cezalandırılmıştır[40]. 5237

---

[38] Sözleşmenin açıklayıcı memorandumu 71. paragraf.

[39] "*Bugün sanal yeraltı dünyasında aynen fizik dünyada yasal herhangi bir ürünün satış öncesi ve satış sonrası hizmetlerine benzer hizmetler verilmektedir. Nitekim istenen bir zararlı yazılımın oluşturulması için "kendin yap" kitlerinden, zararlı yazılımın oluşturulması, yayılması, zararlı etkinin oluşturulması ve menfaatin teminine kadar sürelerde verilen hizmetlere kadar sanal yeraltı dünyası geniş bir yelpazede potansiyel bilişim suç faillerini desteklemektedir. Sanal yeraltı dünyasında sunulan ürünler de geniş bir alana yayılmaktadır. Örneğin bilişim sistemine yetkisiz erişimi sağlayan araçlar, yetkisiz erişim sonucunda elde edilen mali bilgiler, veri kayıtları IP adresleri gibi sayısal varlıklar (digital assets), aynen bir bulut hizmeti gibi belli platformda sunulan bilişim suçlarına ilişkin hizmetler bu kapsamda sayılabilir."*

Bkz. Olgun Değirmenci, "Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi", *Yaşar Hukuk Dergisi*, 1(2), 2019, s. 186.

[40] TCK'da belirtilen hazırlık hareketlerinin cezalandırılması sadece bu suçlarla sınırlı değildir. Örneğin, fuhuş suçunu düzenleyen TCK m. 227 f. 1 hükmünde bu durum, "*Bu suçun işlenişine yönelik hazırlık hareketleri de tamamlanmış suç gibi cezalandırılır*" şeklinde denilmek suretiyle açıkça belirtilmiştir.

sayılı TCK'nın ilk düzenlemesinde ise bilişim suçlarının işlenmesine yönelik hazırlık hareketlerinin cezalandırılmasına yer verilmemişti[41]. Doktrinde de münhasıran bu hazırlık hareketlerinin ayrı bir suç tipi olarak düzenlenmemesi, eleştiri konusu olmuştu[42].

24.03.2016 kabul tarihli 6698 sayılı "Kişisel Verilerin Korunması Kanunu"nun 30. maddesinin 5. fıkrasıyla "Yasak cihaz veya programlar" suçu, TCK'nın İkinci Kısım, Onuncu Bölüm, "Bilişim Alanında Suçlar" başlığı altında, 245/A maddesi olarak şu şekilde düzenlenmiştir:

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

Düzenlenen bu hüküm 07.04.2016 tarihinde yürürlüğe girmiştir[43]. Madde gerekçesinde AK-SSS'nin (Sanal Ortamda İşlenen Suçlar Sözleşmesi) 6. maddesine atıf yapıldığı görülmektedir. Böylelikle sözleşmedeki yükümlülüğün ülkemiz tarafından yerine getirildiğine vurgu yapılmaktadır. Gerekçede hem bilişim suçlarının hem de bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçların caydırıcı ve etkin bir şekilde mücadele ortaya koymak amacıyla bu tür fiilleri suç ve ceza politikası açısından sınırlandırılması ve ceza tehdidiyle yaptırıma bağlanmasında fayda görüldüğü belirtilmektedir. Bu yeni suç tipinin ihdasıyla cezalandırılabilirlik önalana doğru kaydırılmıştır.

Yukarıda da belirtildiği üzere bilişim alanında karşılaşılan gelişmeler dolayısıyla tehditler hem şekil değiştirmiş hem de sayısı artmıştır. Özellikle

---

[41] Yalnızca "Banka veya kredi kartlarının kötüye kullanılması" başlığı altındaki TCK m. 245, f. 2'de yer alan başkalarına ait banka hesaplarıyla ilişkilendirilerek banka veya kredi kartında sahtecilik suçu, TCK m. 245, f. 3'te düzenlenen sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartını kullanmak suretiyle yarar sağlama suçunun hazırlık hareketini oluşturmaktaydı. Bkz. Ahmet Gül, *Doğrudan-Dolaylı Bilişim Suçları*, 3. Baskı, Seçkin Yayıncılık, 2021, s. 250.

[42] Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 8. Baskı, Seçkin Yayıncılık, 2020, s. 484; Aliusta / Benzer, s. 39.

[43] Bkz. 07.04.2016 tarihli, 29677 sayılı Resmi Gazete, <https://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm>, Erişim Tarihi 26 Ekim 2021.

internet kullanımının genişlemesiyle kullanıcıların farkında olmayacağı ve bilgisayarların koruma programlarını kolaylıkla aşabilecek **kötücül yazılımlar** (malicious software "*malware*") da yaygınlaşmıştır[44]. Bu programlar, bilgisayarlara çeşitli şekilde zarar verebilmektedir. İlaveten bu programlar sayesinde bilgisayarın işleyişine herhangi bir zarar vermeksizin de kullanıcıların bilgileri gizli bir şekilde transfer edilebilmektedir. Buna ilişkin tehditler sadece kötücül yazılımla sınırlı değildir, bilakis aygıtlarla birleşebilen donanım veya özel cihazlar aracılığı da karşımıza çıkabilmektedir. Belirtilmelidir ki bilişim suçları; bir cihaz, program, kod ya da şifreye olmaksızın alelade bir bilgisayar kullanılarak da işlenebilir[45]. Ancak TCK m. 245/A hükmünün, içeriği itibariyle **önemli bir boşluğu doldurduğundan bahsetmek mümkündür**[46]. Yukarıda da ifade edildiği üzere, zararlı neticelerin veya tehlike hallerinin gerçekleşmesinin önlenmesi bağlamında bu hükme yer verilmesinin önem arz ettiği sonucuna ulaşılır.

Bu suç tipine ilişkin madde düzenlenmesinin daha doğru bir şekilde yapılmasının mümkün olduğundan bahsedilmektedir[47]. TCK'da genel olarak madde başlıkları düzenlenirken fiil unsuru dikkate alınmaktadır. Bu bağlamda suçun konusunu teşkil eden "yasak cihaz veya programlar" ibaresinin madde başlığı olarak kullanılmasının, kanun sistematiği açısından uygun olmadığına işaret edilmiştir. Aynı sorun TCK m. 200 hükmündeki para ve kıymetli damgaları yapmaya yarayan araçlar suçu bakımından da mevcuttur. Bu doğrultuda her iki hükmün benzer şekilde kurgulandığı sonucuna ulaşmak mümkündür. Buna karşılık ilgili yaklaşımın madde içeriğini yansıtmaktan

---

44 Veli Özer Özbek / Koray Doğan / Pınar Bacaksız, *Türk Ceza Hukuku: Özel Hükümler*, 16. Baskı, Seçkin Yayıncılık, 2021, s. 1021.

45 Şahin Altuğ, "Banka veya Kredi Kartlarının Kötüye Kullanılması", *Uyuşmazlık Mahkemesi Dergisi,* 9(17), 2021, s. 4.

46 Özbek / Doğan / Bacaksız, s. 1021; **Özellikle madde hükmünün banka kartı veya kredi kartlarıyla ilgili işlenen suçlarla mücadelede önem arz ettiğine değinilmiştir. Nitekim Yargıtay kararlarına bakıldığında bilişim suçlarının çoğunluğunun TCK m. 245 hükmü çerçevesinde işlendiği görülmektedir. Bkz.** Metin Turan, *Bilişim Hukuku*, 5. Baskı, Seçkin Yayıncılık, 2021, s. 234, 267; Aynı yönde açıklamalar için bkz. Altuğ, s. 11; Benzer yönde açıklamalar için bkz. Aliusta / Benzer, s. 39.

47 Madde düzenlenmesinin şu şekilde yapılması gerektiği önerilmiştir: "*Bu bölümde düzenlenen suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesinde kullanmak amacıyla bir cihazı, bilgisayar programını, şifre ve güvenlik kodlarını üreten, ithal eden, temin eden satan, satışa arz eden, satın alan veya bulunduran kişi, ….cezalandırılır"*. Bkz. Mahmut Koca / İlhan Üzülmez, *Türk Ceza Hukuku: Özel Hükümler,* 7. Baskı, Adalet Yayınevi, 2020, s. 959.

uzak olduğu belirtilmektedir[48]. Öte yandan madde başlığında **"yasak"** ibaresi bulunmasına rağmen, madde metninde buna yönelik bir ifade yer almamaktadır. Bir cihaz veya programın yasaklı olduğunun belirtilebilmesi için önceden takdir edilen bir yasaklama kararının varlığını gerektirmektedir. Fakat madde metninde, yasaklı olup olmadığına değinilmeden bilişim suçları veya bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen diğer suçlar açısından kullanılan program veya cihazlar dikkate alınmaktadır. Kaldı ki bilişim alanındaki gelişim dolayısıyla yasaklı cihaz ve programların önceden bir liste şeklinde hazırlamak neredeyse imkansızdır. Bu tür nedenlerden dolayı madde başlığının **"*suçta kullanılacak cihaz ve programların üretilmesi, yayılması veya bulundurulması*" şeklinde düzenlenmesi önerilmektedir**[49]. Bu suç tipine kaynaklık eden AK-SSS'nin 6. maddesi de "**cihazların kötüye kullanılması**" şeklinde düzenlenmiştir. Kanaatimizce de madde başlığına yapılan eleştiriler isabetlidir. Bu bağlamda madde başlığının **"program ve cihazların kötüye kullanılması"** olarak değiştirilmesi önerisine iştirak etmekteyiz[50]. Böylelikle "Bilişim Alanında Suçlar" başlığı altındaki diğer suçlarla da uyumluluk sağlanmış olur.

TCK m. 245/A hükmü, "Bilişim Alanında Suçlar" başlığı altındaki bilişim sistemine girme (TCK m. 243), veri nakillerini teknik araçlarla izleme (TCK m. 243, f. 4)[51], sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK m. 244), bilişim sistemi aracılığı ile haksız yarar sağlama (TCK m. 244, f. 4) ve banka veya kredi kartlarını kötüye kullanma suçlarının (TCK m. 245) hazırlık hareketlerini cezalandırılmaktadır. Bu yönüyle madde hükmünün AK-SSS'nin m. 6 hükmüyle uyumlu olduğu ifade edilebilir. Benzer şekilde Al. CK §202c hükmüyle veri casusluğu (§202a) ve verilerin ele geçirilmesi (§202b) suçlarının hazırlık hareketlerinin cezalandırılması öngörülmüştür[52,]

---

48 Özbek / Doğan / Bacaksız, s. 1022.

49 Özbek / Doğan / Bacaksız, s. 1022; Dülger, s. 486.

50 Öneri için bkz. Berrin Akbulut, *Bilişim Alanında Suçlar*, 2. Baskı, Adalet Yayınevi, 2017, s. 348; Aynı yönde Karakurt Eren, s. 223; Kaya / Çakır, s. 39; Bundan başka *Korkmaz,* madde başlığının "*cihaz, program, şifre ve güvenlik kodlarının bilişim suçlarının işlenmesi amacıyla bulundurulması, imal ve ticareti suçu*" olarak düzenlenmesi gerektiğini belirtmiştir. Bkz. İbrahim Korkmaz, "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarını İşlemek Amacıyla İmal ve Ticareti Suçu", *Terazi Hukuk Dergisi*, 13(142), 2018, s. 49.

51 Bu hüküm, 24.03.2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanununun 30. maddesinin 4. fıkrasıyla getirilmiştir.

52 İlgili hüküm, 41. Ceza Kanunu değişikliği (41. Strafrechtsändergungsgesetz-StrÄndG) ile getirilmiştir. Bkz. Bundesgesetzblatt, 07.08.2007, <https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl107s1786.

[53]. Bu hükümle bahsi geçen suçların işlenmesi amacıyla bilgisayar korsanlığı araçlarının imal edilmesi, kendisi veya başkası için tedarik edilmesi, satılması, başkasına devredilmesi, yayılması veya başka bir şekilde erişilebilir kıl**ın**ması suç olarak kabul edilmiştir[54].

Bahse konu suç tipi, yalnızca bilişim suçlarının hazırlık hareketlerini cezalandırmamaktadır. Madde, "*bilişim sistemlerinin araç olarak kullanılması suretiyle*" veya "*bilişim sistemlerinin kullanılması suretiyle*" işlenebilen diğer suçların hazırlık hareketlerini de cezalandırılabilirlik kapsamına almıştır[55]. Bu durumda ilk olarak "*bilişim sistemlerinin kullanılması suretiyle*" nitelikli hırsızlık (TCK m. 142, f. 2, bent e) veya kumar oynanması için yer ve imkan sağlama (TCK m. 228, f. 3) suçları ve "*bilişim sistemlerinin banka veya kredi kurumlarının araç olarak kullanılması suretiyle*" nitelikli dolandırıcılık (TCK m. 158, f. 1, bent f) suçu akla gelmektedir. Esasında bu hükümler

---

pdf%27%5D__1635329751072>, Erişim Tarihi 26 Ekim 2021; 20.11.2015 tarihli Kanun değişikliği öncesi madde hükmü aynen şu şekildedir:

"(1) Her kim 202a veya 202b maddelerinde belirtilen suçların işlenmesine hazırlamak üzere,

1. verilere giriş yapmayı sağlayan (m. 202a fıkra 2) şifre ve sair güvenlik kodlarını veya,

2. bu tür fiilleri işlemeyi amaçlayan bilgisayar programları

üretir, kendisine veya bir başkasına sağlar, satar, bir başkasına verir, yayar veya sair bir şekilde ulaşılabilmesini sağlarsa, bir yıla kadar hapis cezası veya adli para cezası ile cezalandırılır.

(2) 149'uncu maddenin 2. ve 3. fıkraları kıyasen uygulanır." Bkz. Feridun Yenisey / Gottfried Plagemann, *Alman Ceza Kanunu Strafgesetzbuch*, 2. Baskı, Beta Yayınevi, 2015, s. 312.

[53] Söz konusu §202c hükmünün madde başlığı "**veri casusluğunun ve verilerin ele geçirilmesinin hazırlığı**" (Vorbereiten des Ausspähens und Abfangens von Daten) şeklindedir. Madde başlığı bakımından yöneltilen eleştirilerin burada da cari olduğu ileri sürülebilir. Buna karşılık Avusturya Ceza Kanununun §126c hükmünün başlığı "**bilgisayar programlarının veya giriş verilerinin kötüye kullanılması**" (Missbrauch von Computerprogrammen oder Zugangsdaten) şeklinde olup AK-SSS'nin 6. maddesine uyumlu olarak oluşturulmuştur. Bkz. Avusturya Ceza Kanunu, <https://www.jusline.at/gesetz/stgb/paragraf/126c>, Erişim Tarihi 26 Ekim 2021.

[54] Nina Nestler, "Hacker-Tools im StGB", *Juristische Ausbildung,* (6), 2021, s. 629.

[55] Doktrinde "*Bilişim Alanında Suçlar*" başlığı altında yer alan bilişim sistemine girme (TCK m. 243), sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK m. 244) ve banka veya kredi kartlarının kötüye kullanılması (TCK m. 245) suçları "doğrudan bilişim suçları", "bilişim sistemlerinin araç olarak kullanılması suretiyle" işlenebilen diğer suçların ise "dolaylı bilişim suçları" olarak adlandırıldığı görülmektedir. TCK m. 245/A hükmünde düzenlenen suçun da dolaylı bilişim suçu olduğu vurgulanmaktadır. Bkz. Turan, s. 74; Fakat TCK m. 245/A hükmünün de doğrudan bilişim suçu kapsamına girdiği ifade edilmektedir. Bkz. Gül, s. 346 vd.

suçun nitelikli unsuru olarak düzenlenmiştir. Ancak "*bilişim sistemi*" kavramı kullanılmaksızın da hem TCK'daki hem de diğer kanunlarda yer alan bazı suçların bilişim araçları vasıtasıyla işlenebilmeleri pekâlâ mümkündür[56]. Haberleşmenin engellenmesi (TCK m. 124), hakaret (TCK m. 125), haberleşmenin gizliliğini ihlal, (TCK m. 132), kişisel verilerin kaydedilmesi (TCK m. 135), verileri hukuka aykırı olarak verme veya ele geçirme (TCK m. 136), müstehcenlik (TCK m. 226), ses ve görüntülerin kayda alınması (TCK m. 286) gibi suçlar buna örnek oluşturur. Bilişim sistemlerinin kullanılması suretiyle işlenebilen diğer suçların hepsini bu çalışmada zikretmek oldukça güçtür[57]. TCK m. 245/A'daki yer alan "*bilişim sistemlerinin araç olarak kullanılması suretiyle*" ifadesinin yalnızca nitelikli hırsızlık, nitelikli dolandırıcılık ve kumar oynanması için yer ve imkan sağlama suçlarıyla sınırlı olmadığını vurgulamak gerekir. Burada suça ilişkin fiillerin, bilişim sistemleri aracılığı ile işlenmesinin elverişli olup olmadığını araştırmak gerekir. Bu hususlar nazara alındığında TCK m. 245/A hükmünün uygulanma kapsamının AK-SSS m. 6 hükmünden daha geniş olduğu sonucuna ulaşılır[58].

Benzer şekilde Al. CK §263a/3 hükmünde bilgisayar dolandırıcılığı (Computerbetrug) suçunun hazırlık hareketleri cezalandırılmıştır. Ancak bu hüküm AK-SSS'nin 6. maddesi uyarınca düzenlenmiş değildir, bilakis sözleşmenin iç hukuka yansıtılmasından önce 22.12.2003 tarihli Kanun değişikliği ile getirilmiştir[59]. Ayrıca verilerin değiştirilmesi suçunu

---

[56] Kaya / Çakır, s. 39.

[57] Örneğin, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu m. 36 hükmünde yer alan "sahte belge düzenlenmesi" ve m. 37'deki "gerçeğe aykırı beyan, sözleşme ve eki belgelerde sahtecilik" suçları; 5846 sayılı Fikir ve Sanat Eserleri Kanunu m. 71 hükmünde düzenlenen "manevi, mali veya bağlantılı haklara tecavüz" ve m. 72'de mevcut olan koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçları; 5070 sayılı Elektronik İmza Kanunu m. 16'da ihdas olunan "imza oluşturma verilerinin izinsiz kullanımı" ve m. 17'de yer alan "elektronik sertifikalarda sahtekarlık" suçları; Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunun m. 28 hükmünde düzenlenen "izinsiz faaliyette bulunmak", m. 29'da belirtilen "denetim ve gözetim faaliyetlerini engellemek ve istenilen bilgileri vermemek" ve m. 31'de zikredilen "belgelerin saklanması ve bilgi yükümlülüğüne aykırı davranmak" suçları, bilişim sistemlerinin kullanılması dolayısıyla işlenebilmektedir. Bkz. Kaya / Çakır, s. 40.

[58] Maddenin oldukça geniş bir şekilde kaleme alındığına vurgu yapılmıştır. Bkz. Değirmenci, "Cryptolocker…", s. 192.

[59] İlgili hüküm 35. Ceza Kanunu değişikliği (35. StrÄndG) ile getirilmiştir bkz. Bundesgesetzblatt 22.12.2003, <https://www.bgbl.de/xaver/bgbl/start.xav?start=//*%5B@attr_id=%27bgbl103065.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl103065.pdf%27%5D__1633808646777>, Erişim Tarihi 09 Ekim 2021; Keza bu kanun değişikliğine Avrupa Konseyi'nin 25.05.2000 tarihli 2000/383/JHA sayılı

(Datenveränderung) düzenleyen §303a hükmünün 3. paragrafına ve bilgisayar sabotajı suçuna (Computersabotage) yer veren §303b hükmünün 3. paragrafına bakılmalıdır[60]. Bu hükümler ise Al. CK §202c hükmüne atıf yapmaktadır. Dolayısıyla bu suçların da hazırlık hareketleri cezalandırılmaktadır. Bu itibarla Al. CK'nın hem §202c hükmüyle hem de §263a/3 hükmüyle hazırlık hareketleri cezalandırılmaktayken TCK'nın 245/A maddesi tek başına bu ihtiyacı karşılamaktadır[61]. Bu gerekçeyle maddenin belli sınırları ihtiva etmediği ve bu durumun kanunilik ilkesine aykırı olduğu yönündeki eleştirilere[62] **iştirak etmemekteyiz. Aksi takdirde bilişim suçlarının araç olarak kullanılması suretiyle işlenen her suça yönelik Al.** CK'daki gibi ayrı bir madde hükmünün düzenlenmesi söz konusu olurdu. Bu noktada bahse konu suçun TCK'da belirtilen sistemle uyumlu olduğunu ifade etmek mümkündür.

AK-SSS, yukarıda zikrettiğimiz 22.04.2014 tarihli 6533 sayılı Kanunla, 02.05.2014 tarihinde iç hukuka aktarılmıştır. TCK m. 245/A hükmü ise 07.04.2016 tarihinde yürürlük kazanmıştır. Bu iki tarih arasında işlenen fiiller bakımından herhangi bir ceza hukuku sorumluluğu olup olmadığını belirlemek gerekir. Anayasanın m. 90, f. 5 hükmü uyarınca usulüne göre yürürlüğe konmuş uluslararası antlaşmalar kanun hükmündedir. İşaret edilmelidir ki, ceza hukukuna dair hükümler ihtiva eden uluslararası sözleşmeler, temel hak ve özgürlüklere ilişkinse müstakil bir kanuni düzenleme olmaksızın doğrudan uygulamaya konulabilirler[63]. Fakat AK-SSS m. 6 hükmünde bir suç tanımlaması varsa da buna ilişkin bir yaptırım belirtilmemiştir. Bu yüzden

çerçeve kararı kaynaklık etmektedir. Madde hükmü şu şekildedir:

"*(3) Amacı bu madde kapsamına giren fiiller işlemek olan bilgisayar programlarını; imal etmek, kendisi veya başkası için temin etmek, satışa sunmak, bulundurmak veya başkasına bırakmak suretiyle, birinci fıkrada belirtilen suçlardan birini hazırlayan kişi, üç yıla kadar hapis cezası veya adli para cezası ile cezalandırılır*." Bkz. Yenisey / Plagemann, s. 380.

60 İlgili hüküm, 41. Ceza Kanunu değişikliği (41. StrÄndG) ile getirilmiştir. Bkz. Bundesgesetzblatt, 07.08.2007, <https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl107s1786.pdf%27%5D__1635329751072>, Erişim Tarihi 26 Ekim 2021.

61 Doktrinde Al.CK'daki TCK m. 245/A hükmüne karşılık gelecek düzenleme bakımından yapılan açıklamaların eksik olduğu kanaatindeyiz. İlgili çalışmaların birinde m. 245/A hükmüne yalnızca §202c hükmünün benzediği ileri sürülmektedir. Bkz. Karakurt Eren, "Bilişim Alanında…", s. 229. Bir başka çalışmada ise bu suça karşılık olarak münhasıran Al. CK. §263a/3 hükmü gösterilmektedir. Bkz. Kaya / Çakır, s. 41, 42.

62 Korkmaz, s. 52; Aynı yönde, bkz. Karakurt Eren, "Bilişim Alanında…", s. 231; Kaya / Çakır, s. 40.

63 Mahmut Koca / İlhan Üzülmez, *Türk Ceza Hukuku: Genel Hükümler*, 14. Bası, Seçkin Yayıncılık, 2021, s. 52.

TCK m. 245/A hükmünün yürürlüğe konmasından evvel işlenen fiiller ceza hukukuna tabi olmayacaktır[64].

B. Korunan Hukuki Değer

Bilişim suçlarının veya bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen suçların işlenmemesi adına, ön aşamada ceza hukuku müdahalesi mümkün kılınarak bir cihaz, bilgisayar programı, şifre ve sair güvenlik kodunun imal edilmesi, depolanması ve dolaşıma sokulması yasaklanmaktadır[65]. Nitekim bu fiillerin işlenmesiyle bilişim sistemlerinin aksaması, kullanıcıların veri kaybı veya çalınması ve maddi zararın gerçekleşebilme ihtimalleri doğmaktadır.

Korunan hukuki değer bakımından bu suç tipi ile diğer bilişim suçları arasında bir farklılığının bulunmadığı vurgulanmaktadır[66]. Bahse konu suç bakımından korunan hukuki değer, bilişim sistemine duyulan güvendir[67]. Toplumdaki bireyler bu sistemlerin doğru, hatasız ve hızlı bir şekilde işleyebildiğine ilişkin bir güven duyarlar. Suçun işlenmesiyle bireylerin bu güveni sarsılmaktadır. Ne de olsa bilişim sistemleri sayesinde sesli-görüntülü iletişim, elektronik imza, ulusal-uluslararası ticari ilişkiler, internet bankacılığı hizmeti, para aktarımı, elektronik ticaret ve bunun gibi birçok gelişme hayata dahil olmuştur ki buna ilişkin alanların korunmaya muhtaç olduğuna dikkat çekilmektedir[68].

Bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen diğer suçlara yönelik hazırlık hareketlerinin bu madde hükmüyle cezalandırılmasının mümkün hale getirilmesi korunan hukuki değer açısından çeşitli tartışmalara neden olmuştur. Bu durum bu suçla birden fazla hukuki değerin korunduğu ihtimalini gündeme getirmektedir. Belirtildiği üzere bilişim sistemlerine duyulan güven nedeniyle bireyler kendi özel hayatını bilişim alanına açabilmektedir. Bu bağlamda özel hayatın gizliliği hakkının da suçta korunan hukuki değer olduğu ifade edilebilir. Buradan hareket edildiğinde kişinin

---

64 Korkmaz, s. 47.

65 Koca / Üzülmez, *Özel Hükümler*, s. 959.

66 Nestler, s. 630.

67 Koca / Üzülmez, *Özel Hükümler*, s. 960. Bu güven dolayısıyla kişilerin veriler üzerindeki tasarruf yetkisi de korunmaktadır. Benzer durumun Al. CK § 263a/3 hükmü açısından da geçerli olduğuna değinilmiştir. Bkz. Nestler, s. 637.

68 Cengiz Apaydın, "Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu", *Terazi Hukuk Dergisi*, 15(163), 2020, s. 564.

maddi ve manevi varlığını geliştirebilme hakkına (Anayasa m. 5, 17), ilaveten malvarlığı hakkının da korunduğu belirtilerek bu suç bakımından birden fazla hukuki değerin korunduğuna işaret edilmektedir[69]. Diğer taraftan bu suç tipinin bir tehlike suçu olması dolayısıyla asıl olarak toplum güvenliğinin korunduğu belirtilmiştir. Bunun yanında özel hayatın gizliliği, malvarlığı ve haberleşme özgürlüğünün de korunmak istendiğine vurgu yapılmıştır[70]. Kanaatimizce de bu suç dolayısıyla hem bilişim sistemlerine yönelik toplumdaki bireylerin güveni hem de bu araçlarla işlenecek diğer suçlardaki hukuki değerler korunmaktadır[71].

C. Suçun Unsurları

1. Suçun Maddi Unsurları

a. Fail-mağdur

Faillik açısından suç tanımında herhangi bir özellik bulunmamaktadır. Dolayısıyla herkes bu suçun faili olabilmektedir. Bununla birlikte maddede yer alan bazı fiiller, çok failli bir suçu akla getirmektedir. Örneğin, ithal-ihraç, satma-satın alma, verme-kabul etme fiilleri bu bağlamda değerlendirilebilir[72].

Suçun özgü bir suç olmaması dolayısıyla maddede belirtilen fiilleri gerçekleştirilmesi için failin, bilgisayar ya da bilişim alanında uzman bir kişi olmasına gerek yoktur[73]. Buna karşılık doktrinde maddedeki suçları işlemeye elverişli cihaz veya yazılım imal eden kimsenin herkeste olmayan bir uzmanlığa sahip olduğu gerçeğine işaret edilmektedir[74]. Bu noktada uzman bir kişi veya bilgisayar korsanı tarafından bu suçun işlenmesinin suçun nitelikli unsurunun oluşturması gerektiği ileri sürülebilir. Maddede bu yönde bir hüküm bulunmaması nedeniyle bu kişilerin yazılım, cihaz şifre ya da sair güvenlik kodunu imal etmesinin yalnızca cezanın belirlenmesi (TCK m. 61) bağlamında dikkate alınabileceği unutulmamalıdır.

İlgili suç tipi hazırlık hareketlerini cezalandırdığından henüz bilişim

---

69 Özbek / Doğan / Bacaksız, s. 956.

70 Gül, s. 347.

71 Dülger, s. 488.

72 Koca / Üzülmez, *Özel Hükümler*, s. 960. Akbulut, *Bilişim Alanında Suçlar,* s. 350, Dülger, s. 488.

73 Karakurt Eren, "Bilişim Alanında…", s. 225.

74 Kaya / Çakır, s. 44.

sistemlerine yönelen bir saldırı veya bilişim sistemlerinin araç olarak kullanıldığı bir suç söz konusu değildir. Dolayısıyla suçun mağdurunun toplumu oluşturan herkes olduğu belirtilmelidir[75].

b. Suçun konusu

Eşya veya şahsın fiziki veya cismani yönü suçun konusunu oluşturmaktadır[76]. Diğer bir anlatımla tipik hareketin yöneldiği kişi ya da şey, suçun konusunu ifade etmektedir[77]. Esasında maddede bahsi geçen bilgisayar programı, cihaz, şifre veya sair güvenlik kodu fiil araçlarıdır (Tatwerkzeuge)[78]. Fiil araçları, suçun konusuna dahil olsalar da bunlar üzerinde herhangi bir zarar ve tehlike meydana gelmemektedir. Dolayısıyla bilgisayar programı, cihaz, şifre veya sair güvenlik kodunun yanı sıra, bilişim sistemleri de suçun konusunu oluşturmaktadır. Bilişim sistemlerinin araç olarak kullanıldığı diğer suç tipleri göz önüne alındığında, bireylerin malı, özel hayatı ve kişisel verileri de bu suçun konusuna dahil olurlar.

İlgili suç tipinin gerçekleştirilmesiyle bilişim sistemi ve diğer konular üzerinde herhangi bir zarar ya da tehlike ortaya çıkmamaktadır. Dolayısıyla bu suç tipi soyut tehlike suçuna örnek oluşturur[79]. Sırf hareket suçları öncesinde suçlar; sözgelimi "masum" nesneleri bulundurma ve soyut tehlike suçları, hazırlık hareketlerinin cezalandırılmasının başlıca örneklerini oluşturur[80]. Belirtmek gerekir ki, üçüncü kişilerin mevcut cihaz ve programları suç işlemek amacıyla kullanabilme ihtimali, bu hazırlık hareketinin cezalandırılabilmesinin önemli bir göstergesini teşkil eder[81].

Soyut tehlike suçlarında suçun konusu bakımından bir tehlikenin oluşup oluşmadığı hakim tarafından araştırılmamaktadır. Fakat hareketin yapılmasıyla somut tehlike meydana gelmese de esasında bir **tehlike kaynağı (Gefahrenquelle)** yaratılmaktadır. Kanun koyucu, buradaki tehlike

---

75 Koca / Üzülmez, *Özel Hükümler*, s. 960. Akbulut, *Bilişim Alanında Suçlar,* s. 350.

76 İzzet Özgenç, *Türk Ceza Hukuku: Genel Hükümler*, 17. Bası, Seçkin Yayıncılık, 2021, s. 219; Artuk / Gökcen, Çakır / İçer, s. 316.

77 Koca / Üzülmez, *Genel Hükümler*, s.118.

78 Fiil araçları ile ilgili ayrıntılı bilgi bkz. Ünal, "Tehlike Suçları…", s.138 vd.

79 Akbulut, *Bilişim Alanında Suçlar*, s. 349. Apaydın, s. 564. Benzer şekilde Al. CK. 202c hükmünün de soyut tehlike suçu olduğu ifade edilmektedir. Eisele, s. 928; Nestler, s. 629, 630.

80 Bozbayındır, s. 38.

81 Weber, s. 16.

kaynağının oluşumunu genel tehlikeli olarak kabul ederek başlı başına cezalandırma yoluna gitmektedir[82]. Burada cezalandırmayı haklı gösteren tehlikelilik, hazırlık hareketi ile gelecekte gerçekleşen bir zarar eylemi arasındaki ilişkiden ileri gelmektedir[83]. Bu ilişki kurulamıyorsa soyut tehlike suçunun doğru bir şekilde kurgulanmadığı sonucuna ulaşılır. TCK m. 245/A hükmü bu çerçevede değerlendirildiğinde ilgili cihaz, program, şifre ve sair güvenlik kodlarının bilişim suçları ve bilişim sistemlerinin araç olarak kullanılmasıyla işlenen diğer suçlar bakımından bir tehlike kaynağı olduğu açıktır. Bu doğrultuda ilgili haksızlığın, cezaya muhtaç oluşundan bahsetmek mümkündür. Öte yandan hakim, soyut tehlike suçu açısından tehlikenin somut olarak meydana gelip gelmediğini araştırmıyorsa da suçun oluşup oluşmadığı noktasında tehlike kaynakları üzerinde bir araştırma yapabilir. Bu araştırma; ilgili cihaz, program, şifre veya sair güvenlik kodlarının, madde hükmünde belirtilen suçların işlenmesinde, elverişli nitelik taşıyıp taşımadığı ile alakalıdır[84]. Nitekim madde gerekçesinde de bu hususa vurgu yapılmıştır. Şayet bulundurulan cihaz, madde hükmünde belirtilen suçları işlemeye elverişli değilse suçun konusunun yokluğundan bahsedilir. Bu durumda işlenemez suç söz konusu olduğundan failin, suç işleme yönünde kastı dahi olsa ceza hukuku sorumluluğuna gidilmeyecektir[85]. Bu yüzden bunların niteliğinin tespitinde ise uzman bir kişinin görüşüne[86] veya ilgili kurumların raporuna ihtiyaç duyulmaktadır[87].

---

82 Ünal, "Tehlike Suçları…", s. 208, 276.

83 Puschke, s. 12.

84 Al. CK. § 202c hükmünde de bilgisayar programlarının bahsi geçen suçları işlemeye uygun ve bu amaçlı olup olmadığının objektif bir şekilde araştırılması gerekmektedir. Martin Heger, "§ 202c" Kn. 3, in Karl Lackner / Kristian Kühl (Ed.), *Strafgesetzbuch-Kommentar*, 29. Auflage C.H Beck, 2018; Avusturya Ceza Kanununun §126c/2 hükmünde de bu elverişliliğe vurgu yapılmıştır. Buna göre cihaz, şifre ve diğer giriş kodlarının kullanım tehlikesi ortadan kalmışsa bu takdirde faile ceza verilemeyecektir.

85 Tekin, s. 52.

86 Koca / Üzülmez, *Özel Hükümler*, s. 960.

87 Yargıtay bu suça benzeyen para ve kıymetli damgaları yapmaya yarayan araçlar suçu (TCK m. 200) bakımından şu şekilde bir içtihatta bulunmuştur:

" Suça konu ele geçen alet ve malzemelerin TCK.nın 200. maddesi kapsamında para ve kıymetli damgaları yapmaya yarayan araçlar olup olmadığı hususlarında, 5271 sayılı CMK. nın 73. maddesindeki zorunluluk gözetilerek anılan madde hükmü gereğince T.C. Başbakanlık Hazine Müsteşarlığı Darphane ve Damga Matbaası Genel Müdürlüğünden rapor alınarak sonucuna göre sanıkların hukuki durumunun takdir ve tayini gerektiği gözetilmeden,... Kriminal Polis Laboratuvarı Müdürlüğü'nün 02.05.2011 tarihli ekspertiz raporuna dayanılıp eksik araştırma ile sanıklar hakkında yazılı biçimde hüküm kurulması…" Bkz. Yargıtay 8. CD, 2019/1929E., 2021/491K., 18.01.2021, <https://www.sinerjimevzuat.com.

Suç tipinin daha iyi anlaşılması için, suçun konusunun (fiil araçlarının) ayrı ayrı incelenmesi gerekmektedir. Öncelikle cihaz, temel olarak "alet", "aygıt" veya "takım" anlamına gelen bir sözcüktür[88]. Esasında bir donanım unsuruna işaret eden cihaz, cismani bir varlığı belirtir[89]. AK-SSS m. 6/1-a-i hükmünde ise cihazın kapsamına bilgisayar programı da girmektedir. Bununla birlikte sözleşmenin açıklayıcı memorandumunda bilgisayar sistemi, hem donanım hem de yazılım (program)[90] unsurundan oluşan bir cihaz olarak nitelendirilmiştir. Her ne kadar cihaz bir donanım unsurunu belirtse de bu donanım, yazılım olmaksızın çalışmamaktadır. Aynı şekilde donanım olmadan da yazılımın bir hükmü bulunmamaktadır[91]. Kısaca cihaz bir donanım unsuru olarak belirtilse de hem sözleşmede hem TCK'da bu kavramın tanımlanmadığı görülmektedir[92]. Böyle bir tanımın yapılmasına ihtiyaç da yoktur. Zira cihaz kavramının bilişim sistemine bağlanma, eklenebilme ve ihtiyaç duyulduğu takdirde yeniden çıkarılabilir özelliğine sahip bir donanım olduğu noktasında bir kuşku bulunmamaktadır.

Doktrinde bu cihazların ileri teknoloji ürünü olup olmadığı tartışılmaktadır. İleri sürülen bir görüşe göre, suçun işlenebilmesi için cihazların ileri teknoloji ürünü olmasına ihtiyaç bulunmamaktadır[93]. Buna karşılık bir bilişim sisteminin çalışma düzenine normal düzeyde etki eden her araç cihaz kapsamına girmemektedir. Bu bahisle ATM cihazlarında kart ya da para sıkıştırmasında kullanılan saç tokası gibi basit ve sahte kart üretilmesine hazırlanan beyaz plastik kartlar cihaz olarak nitelendirilmemelidir[94]. Önemli olan cihazın bilişim suçlarının ve bilişim sistemlerinin araç olarak kullanılmasıyla işlenen

tr/kullaniciGiris.jsf?dswid=-918#>, Erişim Tarihi 12 Kasım 2021.

88 Türk Dil Kurumu, "Cihaz", <https://sozluk.gov.tr/>, Erişim Tarihi 19 Ekim 2021.

89 Özbek / Doğan / Bacaksız, s. 1023.

90 Kural olarak yazılım, programın bir üst kavramını oluşturmaktadır. Esasında yazılım, program ve veri olmak üzere iki temel unsura dayanmaktadır. Ancak her iki kavram aynı anlamda kullanılmaktadır. Ayrıntılı bilgi için bkz. Osman Gazi Ünal, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" *Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi*, 2011, s. 8.

91 Cihazın donanım ve yazılımı da karşılayan bir ibare olduğu ve bu yüzden zararlı yazılımların da genel olarak bu çerçevede ele alınması gerektiği ileri sürülmektedir. Değirmenci, "Cryptolocker…", s. 190.

92 Kaya / Çakır, s. 43.

93 Özbek / Doğan / Bacaksız, s. 1023.

94 Aksi takdirde cihaz kavramının aşırı şekilde genişleyeceğine vurgu yapılmaktadır. Bkz. Karakurt Eren, "Bilişim Alanında…", s. 224.

diğer suçların gerçekleştirilmesine özgülenmiş olmasıdır[95].

Cihazla ilgili olarak birtakım örneklerden bahsetmek gerekir. Kibrit kutusu boyutunda olan ve "papağan" olarak da adlandırılan okuyucu (reader) cihazı sayesinde, kredi kartı veya banka kartı içindeki tüm veriler kopyalanmakta ve kopyalanan bu bilgiler banka veya kredi kartı sahteciliği için kullanılmaktadır. Bu cihazla elde edilen kart bilgileri kodlayıcı (encoder) adlı cihazla boş bir kartın arkasındaki manyetik kısma yüklenmekte ve bu sayede sahte banka veya kredi kartı imal edilmektedir. Ayrıca ATM'lerin kart giriş kısmına takılan "skimmer" adlı cihazla banka veya kredi kartı bilgileri elde edilebilmektedir. Ancak bu cihazla yalnızca kartın arkasındaki manyetik bilgiler ele geçirildiği için kartın şifresi için ayrı bir cihaza ihtiyaç duyulmaktadır. Bu yüzden ATM'ye sahte klavye (Pinpad) ya da klavyeyi gösteren gizli bir kamera yerleştirilmektedir[96].

Bilgisayar programları, 5846 sayılı Fikir ve Sanat Eserleri Kanununun m. 1/B hükmünün g bendinde,

> "*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 eder."*

şeklinde tanımlanmıştır. AK-SSS'nin 6. maddesinde bilgisayar programından bahsedilmekle birlikte açıklayıcı memorandumda "*istenen sonucu elde etmek için bilgisayar tarafından yürütülebilen bir dizi komut"* **ş**eklinde bir tanımlama yapılmıştır. Temel olarak kullanıcılar, program vasıtasıyla bilgisayarlar üzerinde çeşitli işlemler yapabilmektedirler. Yapılan bu işlemler kötü amaçlı da olabilir. TCK m. 245/A maddesinde bahsi geçen bilgisayar programları ise yukarıda kısmen zikrettiğimiz kötücül yazılımlardır. Bu yazılımlar sayesinde bilişim sistemleri çökmekte, bilişim sistemlerine hukuka aykırı bir şekilde girilmekte verilerin ele geçirilerek başka bir yere transferi gerçekleşebilmekte veya kişinin malvarlığında bir zarar meydana gelebilmektedir. Cihazlarda nasıl ki belirtilen amaçlara ulaşmada bir özgüleme varsa benzer durum bilgisayar programlarında da mevcuttur. Şayet programın niteliğinde bir suça özgülenme durumu anlaşılmıyorsa uygunsuz kullanım da cezai sorumluluk

[95] Özbek / Doğan / Bacaksız, s. 1023.

[96] Genel bilgi için bkz. Akbulut, *Bilişim Alanında Suçlar*, s. 350, 351.

doğurmaz[97]. Buradan hareketle her türlü program kötücül yazılım kapsamına girmemektedir. Virüsler[98], truva atları (trojan horse)[99] mesaj sağanakları (spam)[100], bilgisayar solucanları (worms)[101], arka kapılar (backdoor)[102], klavye dinleme sistemleri/tuş kaydediciler (keylogger)[103], korunmasızlığı

---

97 Eisele, s. 929.

98 "*Kendisinin değiştirilmiş bir kopyasını eklemek için işletim sistemlerini ve programları değiştiren veya çalışmaz hale getiren veya onlara zarar veren programlardır*"

(Akbulut, Bilişim Alanında Suçlar, s. 76). Örneğin, fidye virüsü ile öncelikle hedef bilişim sis temine girilmektedir. Akabinde bilişim sistemine yüklenerek zararlı etki gerçekleştirildikten sonra menfaat temini için farklı teknikler icra edilmektedir. Bu doğrultuda kullanıcının verilerine erişmesi zorlaştırılmakta, hem dosya içeriği ve dosya adı şifrelenebilmektedir. Fidye karşılığında kullanıcılar bu verilere tekrar erişebilmektedir. Bkz. Değirmenci, "Cryptolocker…", s. 178; İlgili fidye, kripto para olarak da istenebilmektedir. Eylem Aksoy Retornaz / Osman Gazi Güçlütürk, *Gelişen Teknolojiler ve Hukuk*, Oniki Levha Yayıncılık, 2020, s. 309.

99 "*…dışarıdan bakıldığında güvenli ve faydalı olarak değerlendirilen ancak görünümünden ve görünürdeki amacından farklı olarak, gizlenmiş olduğu kötü amaç doğrultusunda hareket eden, zararlı ve aldatıcı nitelikteki yazılım programı…*"

Bkz. Engin Erken, in "Truva Atı", in Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021, s. 582.

100 "*Türkçe siber suç ve siber güvenlik literatürüne istenmeyen mesaj olarak kazandırılması amaçlanan spam terimi, "internet üzerinden veya herhangi bir elektronik mesajlaşma sistemi aracılığıyla toplu olarak gönderilen kullanıcı tarafından istenmeyen" mesajlar olarak tanımlanır*".

Bkz. Fatma Saliha Biter, "İstenmeyen Mesaj (Spam)", in Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021, s. 251; Esasında spam mesajlar, kötücül yazılım kapsamına girmezler. Ancak kişinin e-posta hesabını kullanamayacak hale getiren spam mesaj üreten programlar bu suç kapsamında mütalaa edilir.

101 "*Bilgisayar solucanları (worms) bilgisayar sistemlerindeki açık, kusur ve hataları tespit edip kullanıcının herhangi bir eylemine ihtiyaç duymadan kendini yayabilen bir zararlı yazılım (malware) çeşididir."*

Bkz. Cem Eroğlu, "Stuxnet Solucanı Saldırısı-2010", in Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021, s. 526.

102 "*Bir arka kapı, bir bilgisayara veya başka bir sisteme uzaktan erişim sağlamak için kullanılan güvenlik mekanizmalarını atlayan herhangi bir gizli yöntemdir."*

Bkz. Gazi Erkan Bostancı, "Arka Kapı", in Naci Akdemir/Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021, s. 23.

103 "*Tuş kaydediciler (keylogger), klavyede basılan her vuruşu belirli metin dizisi haline getirerek sürekli olarak kaydeder ve ağ üzerinden ya da e-posta olarak kişilere verileri ileten casus programlardır*."

Bkz. Hilal İfaket Akbaş, "Tuş Kaydedici (Keylogger)", in Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021, s. 584.

sömürü haline getiren programlar (exploits)[104], tarayıcı ele geçirmeyi/tarayıcı korsanlığını hedefleyen programlar (browser hijacking-browser hacking)[105], kök kullanıcı takımları/kökset (rootkit)[106] ve casus yazılımlar (spyware)[107] kötücül yazılımlara örnek oluşturur[108, 109]. Bununla birlikte kötücül yazılımların zikredilen örneklerle sınırlı olmadığı aşikardır[110]. Fakat güvenlikle ilgili

[104] Örneğin, Windows işletim sisteminde kullanılan uygulama programının zayıflığı ya da kırılganlığı hakkında bilgileri vermek veya kötücül yazılımları tanıtmak için "sömürü" (exploits) programlarının bulundurulması da suç kapsamındadır. Bkz. Dülger, s. 485.

[105] "*Tarayıcı korsanlığı: Bilgisayar korsanları ve çevrim içi reklamcıların kullandığı web tarayıcısının kontrolünü ele geçirmek için kullanılan bir yöntemdir. Tarayıcı korsanlığı en çok web trafiğini yeniden yönlendirmek, varsayılan tarayıcı ayarlarını değiştirmek veya kurbanı reklamları tıklamaya zorlamak için kullanılır.*"

Bkz. Süleyman Çalışkan, "Ele Geçirme (Hijacking)", in Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021, s. 185; Esasında tarayıcı korsanlığı herhangi bir program imal etmeden de yapılabilir. Fakat bu korsancılığı kolaylaştıran programların üretilmesi bu suç kapsamında ele alınmalıdır.

[106] "*Korsanlık amaçlı programlar adıyla da bilinen kökset (rootkit) istismarı; bir bilgisayar üzerinde çalışan programları gizleyen zararlı bir yazılım olarak sızdıkları hedef bilgisayarda yüklü işletim sisteminin arka planında gizli olarak çalışan programlar dizisini tanımlamak için kullanılan bir terimdir*."

Bkz. Alper Bilgiç, "Kökset (Rootkit)", in Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021, s. 287.

[107] "*Casus Yazılımlar (Spyware): Bulunduğu bilgisayarda kullanıcının izni olmadan kullanıcıya ait bilgileri toplayan bir çeşit zararlı yazılımdır.*"

Bkz. Can Ozan Tuncer, "Zararlı Yazılım (Malware)", in Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021, s. 657.

[108] Akbulut, *Bilişim Alanında Suçlar*, s. 352.

[109] Derin öğrenme teknolojisinin işletilmesiyle sahte medya içeriklerinin imal edilmesi "deep fake" olarak tanımlanmaktadır. İlgili tanım hem sahte medya içeriklerinin imal edilmesi sürecini hem de imal edilen sahte medya içeriğinin kendisi için kullanılmaktadır. Bu yolla orijinal bir videoda yer alan kişinin yüzü tamamen başka bir kişinin yüzüyle değiştirilerek yeni, ancak sahte bir içerik üretilmektedir. Bu sahte içerikler, örneğin sinema sektöründe yararlı olabilmekteyken önemli hukuki değerleri ihlal edebilme potansiyelini taşımaktadır. Ayrıca bu içerikler ulusal güvenliği de tehdit edecek bir biçime bürünebilmektedir. Bkz. Beşir Babayiğit, "Deepfake'in Ceza Hukuku Bakımından Değerlendirilmesi ve De Lege Ferenda Öneriler", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 25(4), 2021, s. 661, 662.

[110] Örneğin, bir bilgisayar programına erişim sağlayabilmek için teknik bir araç olan "USB Dongle"a ihtiyaç vardır. Program bilgisayarda yüklü olsa dahi, programı çalıştıran kodlar USB Dongle'da bulunmaktadır. Yani bilgisayar programı yalnızca bu teknik aracı elinde bulunduran kimse tarafından çalıştırılabilir. Bu araçlar, lisans sahibi tarafından, kullanıcılara belli bir bedel karşılığında satılabilmektedir. Dolayısıyla bu teknik araçları, aşabilecek program tasarlanması da 5846 sayılı Fikir ve Sanat Eserleri Kanununun 72. maddesinde düzenlenen ve özel bir hüküm olan koruyucu programları etkisiz kılma suçunu oluşturur. Bkz.

verileri talep eden kimlik avı e-postalarının (phising) yazılması da bu suçu oluşturmayacaktır[111]. Çünkü bilişim sistemlerine yönelen bazı korsanlık yöntemleri buna özgülenen bir bilgisayar programını gerektirmeyebilir. Örneğin, kişinin hayali bir e-posta uydurarak bu suç anlamında bir hazırlık hareketi ortaya koyduğundan bahsedilemez[112].

Hem TCK'nın "Bilişim Alanında Suçlar" başlığı altındaki suç tanımlarında hem de madde gerekçelerinde şifreye ilişkin bir tanım bulunmamaktadır. AK-SSS m. 6 hükmünde ise şifre, "*bilgisayar şifresi*" olarak, "*bir bilgisayar sisteminin tamamına ya da bir kısmına erişimi mümkün kılan*" şeklinde ifade edilmiştir. Buna karşılık ne sözleşmede ne de sözleşmenin açıklayıcı memorandumunda tanımın içeriğine ilişkin bir açıklama getirilmiştir[113]. Bu noktada literatüre yansıyan genel tanımlara bakmak gerekir. Şifre, bilginin içeriğinin matematiksel algoritmalar kullanılarak karıştırılan bir veri sürecini ifade eder[114]. Daha ayrıntılı bir anlatımla şifre; sayı, harf ya da sembollerden teşekkül eden, gizli kalması belge, bilgi ya da sistemlere erişilmesini mümkün kılan dijital kilitler/anahtarlardır[115]. Şifre sayesinde kullanıcıların bu bilgilere erişmeleri engellenmiş olur. Aynı zamanda karmaşık bir yapıda tasarlanması da mümkündür. Bu durum adli bilişim alanında kolluğun delil elde etmedeki bütün gayretini boşa çıkarabilir[116]. Şifrenin açılması amacıyla tasarlanan "şifre kırıcılar" da bilgisayar programı kapsamındadır. Son olarak şifrenin, suçun işlendiği tarihte güncelliğini yitirmemiş olması gerekir[117]. Yani her zaman bilişim suçlarının ve bilişim sistemlerinin araç olarak kullanılmasıyla işlenen diğer suçların işlenmesine hazır olmalıdır. Aksi takdirde şifrenin suçun işlenmesine özgülenmiş olmasından veya elverişlilik özelliğinden

Olgun Değirmenci, "Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri Suçu", *Terazi Hukuk Dergisi*, 13(140), 2018, s. 114.

111 Bu yöndeki hareket Al. CK § 263a/3 hükmünü uygulamada yeterli değildir. Bkz. Nestler, s. 634. Kanaatimizce bu yönde bir e-posta yazılması, gönderilmesi ve kullanıcının bu e-posta doğrultusunda kimlik veya banka bilgilerini vermesi TCK m. 245/A hükmündeki suçu oluşturmamaktadır.

112 Eisele, s. 926.

113 Karakurt Eren, "Bilişim Alanında…", s. 229.

114 Philip R. Reitinger, "Encryption, Anonymity and Markets", Douglas Thomas / Brian D. Loader (Ed.), *Cybercrime: Law Enforcement, Security And Surveillance In The Information Age,* Routledge, 2003, s. 133.

115 Dülger, s. 483.

116 Reitinger, s. 134.

117 Eisele, s. 928; Aynı yönde bkz. Heger, § 202c Kn. 2, Lackner / Kühl StGB,

bahsedilemeyecektir.

Bilişim teknolojisinde güvenliği sağlamak amacıyla oluşturulan ek ilave kodlara sair güvenlik kodları denilmektedir[118]. Sözleşmenin m. 6/1-a hükmünde bu kısım "*erişim kodu veya benzeri bir veri"* **şeklinde belirtilmiştir. Şifre dışında kullanıma tahsis edilen parmak izi, ses, retina ya da avuç içi tanıma (**biyometrik tanıma) gibi nitelikleri içeren güvenlik unsurları sair güvenlik kodlarına örnek oluşturur[119]. Bundan başka kredi kartlarının arkasında yer alan CVV, CVV2 ve CVC2 gibi kodlar[120] da sair güvenlik kodlarına dahildir. Sair güvenlik kodları verilen örneklerle sınırlı değildir. Bu yüzden kanun koyucu, "*sair güvenlik kodu*" şeklinde bir ibareye başvurarak ismi farklı olsa da tüm güvenlik kodlarını kapsam altına alma amacını gütmüştür[121]. Bununla birlikte bilişim sistemlerinin gelişimiyle yeni güvenlik kodları da üretilmektedir. Örneğin "karekod" uygulaması sayesinde resmi belgeler de sorgulanabilmektedir. Şifrenin de bir güvenlik kodu olduğu ve bilişim sistemine girmek amacıyla tasarlandığı göz önüne alındığında, maddedeki "***şifre veya sair güvenlik kodu***" ibaresinin "belirlilik" ilkesine aykırı olduğu görüşüne katılmamaktayız[122]. Nitekim maddedeki "sair" ifadesinin "şifre veya sair" ifadesiyle birlikte ele alınması gerekmektedir[123].

c. Fiil

Suçun konusunu "*imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran*" şeklinde madde metninde belirtilen hareketlerin herhangi birinin icra edilmesiyle suç tamamlanmış olur. İlgili suçun seçimlik hareketli suç olduğu noktasında herhangi bir kuşku bulunmamaktadır[124]. Bu suça dair hareketlerden birkaçının veya hepsinin gerçekleşmesi halinde de suçun bir

[118] Akbulut, Bilişim Alanında Suçlar, s. 353.

[119] Dülger, s. 489.

[120] Bu kodlar kredi kartı şifresinden farklılık arz eder. Bkz. Apaydın, s. 566.

[121] Akbulut, Bilişim Alanında Suçlar, s. 353.

[122] Özbek / Doğan / Bacaksız, s. 1025; Aynı yönde bkz. Korkmaz, s. 51; Aksi görüş için, Kaya / Çakır, s. 44.

[123] Koca / Üzülmez, *Özel Hükümler*, s. 960; Al. CK § 202c hükmünde yer alan "*verilere giriş yapmayı sağlayan*" ifadesiyle şifre ve sair güvenlik kodunun kapsamının sınırlandırmış olduğu belirtilmektedir. Bu yönüyle ilgili düzenlemenin AK-SSS m. 6 hükmüne benzer olduğu söylenebilir. Bkz. Karakurt Eren, "Bilişim Alanında…", s. 229.

[124] Koca/Üzülmez, *Özel Hükümler,* s. 960; Özbek / Doğan / Bacaksız, s. 1025; Akbulut, *Bilişim Alanında Suçlar*, s. 355; Dülger, s. 489; Altuğ, s. 5.

defa işlenmiş olduğu sonucuna ulaşılır. Fakat seçimlik hareketlerden her birinin aynı konuya yönelmesi gerekmektedir. Burada tür bakımından bir ayniyet değil, bilakis nesnel olarak bir ayniyet aranmaktadır. Aksi takdirde seçimlik hareketli bir suçtan bahsedilemez[125]. Örneğin, fail bir yandan bankanın bilişim sistemine girebilmek amacıyla bir program imal edebilirken diğer yandan kredi kartı kopyalamak amacıyla bir cihaz satın alabilmektedir. Suçun konuları nesnel olarak aynı olmadığı için fail iki ayrı yasak cihaz veya program bulundurma suçundan ayrı ayrı cezalandırılmalıdır. Buna karşılık failin, aynı türdeki cihazları depoladıktan sonra başka bir yere naklederek satışa arz etmesi durumunda tek suçun oluştuğundan bahsedilmelidir. Birden fazla kez seçimlik hareketlerin gerçekleştiği göz önüne alındığında bu durum, cezanın belirlenmesinde (TCK m. 61) dikkate alınabilir[126].

Maddede seçimlik hareketler tek tek belirtildiği için bunların haricinde bir fiilin gerçekleştirilmesiyle suç işlenmiş sayılmaz[127]. AK-SSS m. 6/1/a hükmünde "**tedarik etme**" ifadesine yer verilmiştir. Geniş anlamda bu ifade yapım, satım veya kullanılmak üzere satın alma, dağıtım hareketlerini belirtmektedir[128]. Aynı şekilde sözleşmedeki "**başka bir şekilde erişilebilir hale getirme"** ifadesi ise hareketi oldukça genişletmektedir[129]. TCK m. 245/A hükmünde bu yönde bir ifadeye yer verilmediği gibi kanunilik ilkesine uygun olarak seçimlik hareketler tek tek zikredilmiştir[130]. Buna karşılık sözleşmede kullanılan ifadenin bilgisayar teknolojisinde gerçekleşebilecek yeni gelişmeleri de kapsayabileceğine vurgu yapılmıştır[131]. Her ne kadar TCK m. 245/A hükmünde belirtilen seçimlik hareketlerin tek tek sayılması kanunilik ilkesiyle uyumlu olsa da bunların fazla ve geniş yapıda olmaları dolayısıyla teknolojik gelişmeleri karşılayabileceği kanaatindeyiz.

Doktrinde "**yayma**" hareketinin bulunmaması eleştirilmekte ve bu hareketin madde metninde yer almasının suçla mücadele için önemli

125 Özgenç, s. 186.

126 Koca / Üzülmez, *Özel Hükümler*, s. 961.

127 Özbek / Doğan / Bacaksız, s. 1026.

128 Dülger, s. 489.

129 Bu yönüyle Al. CK §202c hükmünün, seçimlik hareketler bakımından sözleşmeyle büyük bir uyum sağladığı ifade edilebilir. Buna karşılık Al. CK §202 hükmünde de "başka bir şekilde erişilebilir hale getirme" (sonst zugänglich machen) ifadesi yer almakla birlikte Al. CK §263/a/3 hükmünde böyle bir ifadeye yer verilmemiştir.

130 Akbulut, *Bilişim Alanında Suçlar*, s. 346.

131 Korkmaz, s. 48.

olduğuna dikkat çekilmektedir[132]. Buna karşılık aşağıda inceleyeceğimiz üzere "nakletme" ve "sevk etme" seçimlik hareketlerinin "yayma" hareketini kapsadığını düşünmekteyiz[133]. Yine doktrinde, "sevk etme" ile "nakletme", "depolama" ile "bulundurma" hareketlerinin, aynı veya yakın anlamlarda olduğu ve bu yüzden aynı suç tanımında benzer ifadelere yer verilmesinin isabetli olmadığı belirtilmektedir[134].

Maddedeki seçimlik hareketlerin ayrıntılı bir şekilde değerlendirilmesi gerekmektedir. "İmal etme" bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun kullanılabilir şekilde fiili olarak üretilmesi anlamına gelmektedir[135]. Fiziki araç ve gereçler sistemli bir şekilde bir araya getirilerek cihazın üretilmesi mümkündür. Bunun için devre, kablo ve hafıza kartları gibi daha önceden üretilen ürünlerin kullanılması da imal etme seçimlik hareketi kapsamındadır. Önemli olan cihazların kendisini meydana getiren parçalardan bağımsız ve yeni bir bütünlük oluşturmasıdır. Madde hükmünde belirtilen suçları işlemek amacıyla programlar da imal edilebilmektedir. Bu kapsamda yeni bir program imal edilebileceği gibi mevcut bir programın bir çeşidi de üretilebilir[136]. İmal edilen program zamanla niteliğini, yani bir bilişim suçunu işleme elverişliliğini kaybedebilir. Bu yüzden elverişliliği sağlayacak biçimde programın daha üst bir sürüme güncellenmesi de imal kapsamındadır. Bu güncellenmeler, belirli dönemlerde de gerçekleştirilebilir. Dolayısıyla elverişliliğinin kaybolmaması adına, belirli dönemlerde tekrar eden güncelleme, imal etmenin temadi eden bir fiil gibi görünmesine neden olur. Fakat böyle bir dönem öngörülmemişse ve uzun bir zaman sonra program güncellenmişse bu durumda yeni bir fiil işlenmiş olacaktır. Öte yandan yukarıda bahsedildiği üzere "şifre kırıcılar" bir bilgisayar programıdır. Ancak şifre oluşturucu programlar vasıtasıyla şifreler de imal edilebilmektedir. Nitekim, bu programlar sayesinde şifre üretilerek lisanslı yazılımlara

---

132 Akbulut, *Bilişim Alanında Suçlar*, s. 357.

133 Benzer yönde bir görüş için bkz. Dülger, s.489.

134 Koca / Üzülmez, *Özel Hükümler*, s. 961; Bu seçimlik hareketlerin farklı anlamlar taşıdığına ilişkin görüş için bkz. Korkmaz, s. 52.

135 Akbulut, *Bilişim Alanında Suçlar*, s. 355.

136 Özbek / Doğan / Bacaksız, s. 1025; Örneğin, özel bir hüküm olan 5846 sayılı Kanunun 72. maddesindeki koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçunda bu amaçla üretilmeyen bir programın kaynak kodlarının değiştirilmesi suretiyle de koruyucu programları etkisiz kılacak elverişliliğe kavuşturulması imal kapsamındadır. Ayrıntılı bilgi için bkz. Değirmenci, "Koruyucu Programlar…", s. 114.

erişilebilmektedir[137].

"İthal etme" cihaz, program, şifre veya sair güvenlik kodunun yurt dışından ülkeye aktarılması anlamına gelmektedir. Cihazlar yurt dışından ülkeye ithal edilebilir. Fakat cihaza ilişkin parçaların ayrı ayrı ithal edilip bunların ülkede birleştirilmesinin ithal etme kapsamında olmadığını belirtmek gerekir. Program, şifre veya sair güvenlik kodlarının taşınabilir bir bellek veya akıllı kart içerisinde ülkeye getirilmesi ithal etme fiili kapsamındadır. Bununla birlikte yurt dışındaki bir kullanıcının veya içerik sağlayıcısının dijital ortama aktardığı program, şifre veya sair güvenlik kodunun bedeli ödenerek ithali de mümkündür. Bu bahisle ithal için mutlaka sınır kapısı geçişinin aranmasına gerek olmadığına vurgu yapılmaktadır[138]. Bilişim sistemlerinin sınır aşan özellikleri göz önünde alındığında ithal etme hareketinin, klasik anlamla sınırlı kalmayacağı ortadadır[139]. Ancak yurt dışındaki dijital ortamdan program, şifre veya sair güvenlik kodlarının tedarik edilmesinin ithal etme kapsamında olmadığı, bunların aşağıda inceleneceği üzere kabul etme veya satın alma seçimlik hareketi içerisinde değerlendirilmesi gerektiği fikri de ileri sürülebilir.

"Sevk etmek", madde hükmü bağlamında cihazın, bilgisayar programının şifre veya sair güvenlik kodunun bir yerden başka bir yere aracı yoluyla gönderilmesini ifade eder. Benzer şekilde **"nakletmek",** bahsi geçen suçun konularının bizzat fail tarafından taşınması veya aktarılması anlamına gelmektedir. Bu hareketlerin mutlaka dış dünyada gerçekleşecek şekilde yapılması gerekmeyip bilişim alanında da icra edilmesi mümkündür. Öte yandan ithal etmenin aksine ihraç etmek, madde metninde yer almadığı için sevkin veya nakletmenin yurt içinden veya yurt dışından yapılmasının bir öneminin bulunmadığına vurgu yapılmaktadır[140].

"Depolama ve bulundurma" seçimlik hareketleri yukarıda da zikredildiği üzere hemen hemen aynı anlamlara gelmektedir. Bu hareket, bir cihazın, programın, şifrenin veya sair güvenlik kodunun istendiği takdirde erişilebilecek yerde bulundurulmasını ifade etmektedir. Her ikisinde de bir fiili hakimiyet durumundan bahsedilmelidir. Bu hakimiyet bakımından zilyetlik

137 Nestler, s. 632.

138 Özbek / Doğan / Bacaksız, s. 1025.

139 Kaya / Çakır, s. 45.

140 Akbulut, *Bilişim Alanında Suçlar*, s. 356.

yeterli olup mülkiyet ilişkisinin varlığı aranmaz[141]. Fiili hakimiyet dolayısıyla bu seçimlik hareketler, temadi özelli**ği göstermektedir. Böylelikle cihaz, program, şifre veya sair güvenlik kodları elde bulundurulduklarısüre içerisinde suç işlenmeye devam etmektedir. Suçun işlendiği zamanın tespiti ve zamanaşımının başlangıcı bu bağlamda önemlidir**[142].

AK-SSS m. 6 hükmüne göre, taraf devleler, özellikle depolama/bulundurma hareketi bakımından cihaz, bilgisayar programı, şifre veya güvenlik kodunun belli sayıda bulundurulmasını suçun oluşması yönünden bir koşul olarak ileri sürebilirler. Zira suçun konuları üzerinde depolama/bulundurma hareketinin, suç kapsamına alınmasıyla uygulamada birtakım ispat sorunlarının ortaya çıkabileceğine değinilmektedir[143]. Buna karşılık TCK m. 245/A hükmünde bu yönde bir tasarrufun olmadığı görülmektedir. Kanaatimizce burada sayıdan ziyade depolanan/bulundurulan cihaz, program, şifre veya sair güvenlik kodunun özgülenme ve niteliğine bakılarak bir yargıya varılmalıdır.

Cihazlar bakımından depolama/bulundurma bir sorun teşkil etmemektedir. Program, şifre veya sair güvenlik kodlarının bir bellek cihazına kaydedilmesi de aynı anlama gelmektedir. Fakat her kaydetme depolama/bulundurmayı ifade etmemektedir[144]. Zira bulut bilişim alanına da kayıt yapılabilir. Aslında bu kayıt "yükleme" olarak adlandırılır. Bu durumda depolamadan bahsedilmese de sevk veya nakletmeden söz edilebilir. Ayrıca depolama/bulundurma için yapılan kaydın niteliği, boyut ve amacı gibi hususların da nazara alınması gerektiğine işaret edilmektedir[145].

"Satmak" tarafların önceden kararlaştırdıkları meblağ karşılığında cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun alıcıya transfer edilmesidir. "**Satın almak"** ise bedel karşılığında maddede yer alan suçun konularının alınmasını ifade eder. Önemli olan alıcının, cihaz veya programa erişim sağlamasıdır. Örneğin, suça konu program elde edilirken programa giriş yapan güvenlik kodu bilgisine de sahip olunmalıdır[146]. Aksi takdirde erişim sağlayamadığı cihaz veya program dolayısıyla fail ancak

[141] Akbulut, *Bilişim Alanında Suçlar*, s. 357.

[142] Koca / Üzülmez, *Özel Hükümler*, s. 961.

[143] Erdem / Özocak, s. 188.

[144] Akbulut, *Bilişim Alanında Suçlar*, s. 356.

[145] Özbek / Doğan / Bacaksız, s. 1026.

[146] Eisele, s. 929.

bulundurma seçimlik hareketi uyarınca cezalandırılacaktır. İlaveten failin, cihaz veya programı erişim sağlayabilecek bir başka kişiye de satabileceği ihtimali unutulmamalıdır. "**Satışa arz etmek"** ise bir malın satış yapılabilecek şekilde piyasaya sürülmesini ifade eder. İlgili cihaz, program, şifre veya sair güvenlik kodlarının satılmasına yönelik bir iradenin ortaya çıkarılması bu seçimlik hareket bakımından önemlidir[147]. Bu irade üreticinin satış politikası veya reklamlarıyla da ortaya konulabilir. Maddede belirtildiği üzere satışa arz da başlı başına cezalandırılmaktadır. Esasında satmak açısından satışa arz, teşebbüs aşamasında kalan bir diğer seçimlik hareketi göstermektedir[148]. Bu hareket teşebbüs aşamasında kalan hareketin tamamlanmış suç gibi cezalandırılmasını öngörmektedir[149].

"Kabul etmek", bahsi geçen suçun konularının belli bir ücret karşılığı olmadan sağlanmasını gösteren bir başka seçimlik harekettir. Satın almak arasındaki farkı bunun bir ticari ilişki olmadan yapılmasına dayanmaktadır. Kabulün sürekli ya da geçici olmasının veya daha sonra cihazın iade edilme ihtimalinin, suçun oluşumu üzerinde bir etkisi yoktur. Bununla birlikte **"başkasına vermek"** ise satış işlemi olmadan suçun konularının bir başkasının kullanımını mümkün kılan bir teslim işlemidir. Bu seçimlik hareket, cihazların elden çıkarılması gibi dış dünyaya yansıyan şekilde gerçekleşebileceği gibi program, şifre veya sair güvenlik kodunun dijital ortamı üzerinden de icra edilmesi mümkündür. Bedel karşılığı olmaksızın temin fiillerinin cezalandırılmasında bu seçimlik hareketin TCK'nın 245/A maddesinde yer alması, ortaya çıkabilecek hüküm boşluğunun doldurulması bağlamında önemlidir[150].

2. Suçun Manevi Unsurları

Bu suç kasten işlenebilen bir suç olup taksirle işlenmesi öngörülmemiştir. Fail ilgili seçimlik hareketleri gerçekleştirirken cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun suçun konusu kapsamında olduğunu bilmelidir[151].

---

147 Özbek / Doğan / Bacaksız, s. 1027.

148 Akbulut, *Bilişim Alanında Suçlar*, s. 360.

149 Satışa arz seçimlik hareketinin AK-SSS m. 6 maddesinde taraf devletlere yönelik suç haline getirme yükümlülüğünün kapsamını aştığı ifade edilerek orantılılık ve son çare olma ilkesi ile bağdaşmadığına vurgu yapılmaktadır. Bkz. Karakurt Eren, "Bilişim Alanında…", s. 234.

150 Karakurt Eren, "Bilişim Alanında…", s. 234, 235.

151 Örneğin, suçun konusu hakkında bilgi sahibi olmayan bir kimse, başkaları tarafından imal edilen veya oluşturulan bir cihazı failin isteği doğrultusunda naklederse, bu kimse bakımından ceza hukuku sorumluluğu doğmayacaktır. Gül, s. 349; Benzer şekilde eve gelen misa-

Fakat kastın varlığı bu suçun oluşması için yeterli olmayıp kastın yanında amaç unsurunun da bulunması gerekir[152]. AK-SSS m. 6 hükmünde de bu manevi unsura vurgu yapılmıştır[153]. Buna göre sözleşmenin 2. ve 5. maddeleri arasında sayılan suçların işlenmesi **"maksadıyla"** ilgili fiiller icra edilmelidir. Aksi takdirde manevi unsur gerçekleşmediğinden suç oluşmayacaktır.

Amacın objektif olarak tezahür etmesi gerekmektedir[154]. Bu doğrultuda bir bilgisayar sisteminin test edilmesi veya korunmasının amaçlandığı hallerde ceza sorumluluğu doğmayacaktır. Bir diğer ifadeyle hem suçların işlenmesi hem de meşru amaçlar için kullanılabilecek çift kullanım**lı**[155,156]

---

firin suçun konusunu unutması halinde ev sahibi tarafından bu kişiye ulaştırılmasına kadar geçen zamanda ev sahibinin suçu işlemeye yönelik kastından söz edilemez. Altuğ, s. 31.

[152] "*Hazırlık suçlarının çoğu zaman eyleme uzak olması ve buna bağlı olarak planlanan eylemin düşük düzeyde somutlaşması karşısında yeterli ölçüde bir sübjektif haksızlık içeriği, birçok durumda yalnızca gelecekteki eyleme yönelik amaç ya da bilme şeklindeki nitelikli bir kastın varlığı ile gerekçelendirilebilir."*

Bkz. Sieber, s. 448.

[153] Suçun konusu olan cihazların suç işlemek amacıyla imal edilmesi yeterli görülerek objektif unsurlar yerine, sübjektif unsurlara yer verildiğinden bahsedilmektedir. Değirmenci, "Koruyucu Programlar…", s. 114.

[154] Sieber, s. 448.

[155] Çift kullanımlı eşyalar kapsamına; TCK m. 174 hükmünde yer alan tehlikeli maddelerin izinsiz olarak bulundurulması veya el değiştirilmesi suçu, TCK m. 188 hükmündeki uyuşturucu veya uyarıcı madde imal ve ticareti suçu ve para ve kıymetli damgaları yapmaya araçlar (TCK m. 200) suçlarının konuları da girmektedir. Yalnız bu suçların konusunu oluşturan eşyaların veya maddelerin hukuka uygun amaçlar doğrultusunda kullanılabilmeleri, yetkili bir merciin izin veya ruhsatı doğrultusunda mümkün olurken böyle bir durum TCK'nın 245/A maddesinde öngörülmemiştir.

[156] Çift kullanımla ilgili olarak Al. CK. § 202c hükmü Anayasa şikayetine (Verfassungsbeschwerde) konu olmuş ve hak ihlali yapıldığı ileri sürülmüştür. Anayasa şikayetine başvuran kişi teknik bir üniversitede bilişim alanında profesör olarak görev yapan bir bilim adamıdır. Başvurucu, bilişim sistemlerinde olası zayıf noktaları izlemek için sistematik testler kullanan ve bu boşlukların güvenlik analizini yapan programlar hazırlamıştır. Başvurucu derste kullanılan programları öğrencilerin indirebilmeleri için ana sayfada yayınlamıştır. Böylelikle üçüncü kişiler de bu programlara erişim imkanına kavuşmuştur. Fakat başvurucu başka kişilerin kullandıkları bilgisayarların güvenlik önlemlerini aşarak onlara erişmelerinin kabul edilemez olduğunu derslerinde özellikle vurgulamıştır. Başvuruda, madde hükmüne yalnızca bilgisayar suçlarının işlenmesine elverişli programların girmediği federal hükümet tarafından ifade edilmişse de bu ayrımın kanuni metne yansıtılmadığı ve Anayasanın § 103/2 hükmünün ihlal edildiği ileri sürülmüştür. Anayasa mahkemesi, AK-SSS hükümlerine atıf yaparak, ilgili programların çift kullanımlı olduğuna dikkat çekerek, somut olayda amacın bunların öğrenciler tarafından öğrenilmesindeki genel yararı da nazara alarak ilgili düzenlemenin bir hak ihlali oluşturmadığına hükmetmiştir. Özellikle çift kullanımlı cihaz veya programlar bağlamında sadece programın bahsi geçen suçları işlemeye elverişli oluşuyla yetinmenin isabetli olmadığına değinilmiştir. İlgili Anayasa şikayeti için bkz. Bundesver-

cihaz veya programlar bu suç kapsamına dahil edilmemelidir. İlaveten bankacılık sistemlerinde veya sağlık sisteminin bilişim alanlarına yönelik güvenlik açıklarına dikkat çekmek ve böylece onların ortadan kaldırılmasına katkıda bulunulması da bu amaç kapsamına girmemektedir[157]. Buna karşılık bilgisayar korsanlığına uygun cihaz ve program ile hukuki çerçevede kullanımı arasındaki çizginin nerede olduğunun belirsizlik içinde kaldığına vurgu yapılmaktadır. Öyle ki sızma testi programlarını nezdinde bulunduran kişilerin, hukuka uygun amaçlar doğrultusunda bunları bulundurduklarını ispat noktasında güçlük yaşamaları muhtemeldir[158]. Bu noktada program ve cihazın kökenine, kullanım bağlamlarına ve kullanıcısı tarafından izlenen hedeflere bağlı olarak hem hukuka uygun hem de suç işlemeye ilişkin amaçlara hizmet edebileceğine işaret edilmektedir. Fakat klasik bilgisayar korsanlığı cihaz ve programlarının bunun içerisinde olmadığı ortadadır[159]. Çift kullanımlı cihaz ve programların belirsizliğine rağmen suçun maddi unsurları temelinde tatmin edici bir çözüm getirilmesinin mümkün olduğu belirtilmektedir[160].

Fail, bilişim suçlarının ve bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenebilmesi amacıyla madde hükmünde belirtilen seçimlik hareketleri icra etmelidir. Amaç veya saik gibi manevi unsurlar ise hazırlık hareketlerini cezalandıran soyut tehlike suçlarını sınırlamada önemli fonksiyon üstlenmektedir. Dolayısıyla soyut tehlike suçlarında herhangi bir hareket değil, belli bir amaçla icra edilen hareket cezalandırılmaktadır[161]. Aynı zamanda çift kullanımlı cihaz ve programların özellikle depolama/bulundurma seçimlik hareketleri bağlamında sınırlandırılması açısından da amaç unsuru ön plana çıkmaktadır[162,163].

---

fasssungsgericht, Beschluss vom 18.05.2009, 2 BvR 2233/07, <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/05/rk20090518_2bvr223307.html>, Erişim Tarihi 16 Kasım 2021.

157 Nestler, s. 613, 631, 632.

158 Erdem / Özocak, s. 189.

159 Nestler, s. 637.

160 Örneğin, failin üçüncü bir kişinin bahse konu diğer suçlar için kullanılacağını kabullenmesi halinde ortalığa bir parola bırakarak da erişim sağlanabilmektedir. Bkz. Eisele, s. 930.

161 Ünal, "Tehlike Suçları…", s. 328.

162 Eisele, s. 929.

163 *Babayiğit;* örneğin, bilişim sistemlerinin araç olarak kullanılması suretiyle nitelikli dolandırıcılık suçunu işlemek amacıyla "deepfake" içerik imal eden bir program bulundurulmasının TCK m. 245/A hükmü kapsamına girdiğini, ancak salt deepfake içerik imal eden her programın bu suç dahilinde olmadığını ifade etmektedir. Bkz. Babayiğit, s. 666; Yazar

TCK m. 245/A hükmü dahilinde **böyle bir amaç unsuruna yer verilmesi** cezalandırılabilirlik alanının sınırlandırılması bağlamında isabetlidir.

Madde hükmünde amaç unsuruna yer verilmesi suçun ancak doğrudan kastla işlenebileceğini göstermektedir[164]. Benzer yönde Al. CK. §202c hükmü düzenlenirken Alman kanun koyucusunun AK-SSS'nin asgari gerekliliklerini aşarak daha katı bir sorumluluk öngördüğüne değinilmektedir[165]. Dolayısıyla Al. CK. §202c hükmünün de doğrudan kastla işlenebileceğine vurgu yapılmaktadır[166, 167]. Kanaatimizce de bu suçun olası kastla işlenmesi mümkün değildir. Bu sebeple, suçun olası kastla işlenebileceğini belirten görüşe[168] iştirak etmemekteyiz.

Bu suç bakımından hata hükümlerinin (TCK m. 30, f. 1) uygulanması mümkündür. Örneğin bu suç kapsamındaki bir program yanlışlık veya dikkatsizlikle internet ortamından indirilmiş olabilir[169]. Bu durumda failin bu suça yönelik kastının olmadığı ortadadır. Suçun taksirli hali de düzenlenmediğinden failin ceza hukuku sorumluluğuna gidilemeyecektir.

---

burada amaç unsurundan hareket etse de yukarıda da belirtildiği üzere bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların yalnızca nitelikli hırsızlık, nitelikli dolandırıcılık ve kumar oynanması için yer ve imkan sağlama suçlarıyla sınırlı olmadığını vurgulamak gerekir. Örneğin, sahte içerik üreten programlar sayesinde şantaj (TCK m. 107, f. 2) ve kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçları (TCK m. 136) da işlenebilmektedir. Bu yüzden "deepfake" içerik üreten programlar, TCK m. 245/A hükmündeki suçun konusu dahilindedir. Bu çerçevede, bahsi konu programın ilgili suçların işlenmesine özgülenip özgülenmediğine ve failin bu suçları işleme amacı taşıyıp taşımadığına bakılmalıdır.

164 Artuk / Gökcen / Alşahin / Çakır, s. 466; Dülger, s. 490; Karakurt Eren, "Bilişim Alanında…", s. 237. Benzer nitelikteki suçlar için bkz. Koca / Üzülmez, *Özel Hükümler*, s. 60, 439, 634.

165 Eisele, s. 929, 930.

166 Esasında bu durumun 1. dereceden kasta vücut verdiği (Absicht) belirtilmektedir. Fakat buradaki amaç unsurunun bilgisayar programına atıfta bulunduğuna, bilgisayar programının nesnel öğesinin bir parçası olarak anlaşıldığına işaret edilmektedir. Bkz. Nestler, s. 633; Eisele, s. 930; Buna karşılık suçun olası kastla işlenebilmesinin mümkün olduğuna da değinilmektedir. Bkz. Heger, "§ 202c Kn. 5", Lackner / Kühl, StGB; Sieber, s. 301, 444.

167 Öte yandan Al. CK. § 263a/3 hükmünde belirtilen suçun olası kastla işlenmesinin yeterli olduğuna vurgu yapılarak doğrudan kast doğrultusunda düzenleme yapılması gerektiği belirtilmektedir. Bkz. Nestler, s. 634.

168 Akbulut, *Bilişim Alanında Suçlar*, s. 358; Özbek / Doğan / Bacaksız, s. 1028; Apaydın, s. 567.

169 Eisele, s. 929.

3. Hukuka Aykırılık Unsuru

Suçun diğer bir unsurunu oluşturan hukuka aykırılıkta tipe uygun fiil, tüm hukuk düzeni açısından ele alınmakta ve fiilin işlenmesinin hukuka uygun olup olmadığı değerlendirilmektedir. Fiile ilişkin somut olayda bir hukuka uygunluk nedeni gerçekleşmemişse fiilin suç teşkil ettiğinden bahsedilir[170]. Bu suç tipiyle ilgili olarak görevin ifası ve ilgilinin rızası hukuka uygunluk nedenlerinin incelenmesi gerekmektedir[171].

Öncelikle 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 girip girmediğini değerlendirmek gerekir. CMK m. 134, f. 1 hükmü uyarınca bir suç dolayısıyla başlatılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil etme imkanının bulunmaması halinde şüphelinin kullandığı bilgisayar ve bilgisayar programları ile kütüklerinde arama yapılabilir kopya çıkartılabilir ve ilgili kayıtlar çözülerek metin haline getirilebilir. Bu maddenin ikinci fıkrasına göre ise bilgisayara, bilgisayar programlarına ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi ve gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde, çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için bu araç ve gereçlere elkonulabilecektir. Şifrenin çözülmesinde adli bilişim uzmanları buna uygun özel programları kullanabilmekte, çözümünün yapılması ve gerekli kopyaların alınması halinde elkonulan birimlerin gecikme olmaksızın iadesi yapılabilmektedir[172]. Bu bahisle şifre kırıcı programların veya cihazların bulundurulması, sağlanması veya imal edilmesi hukuka aykırılık kapsamında görülemez[173]. Diğer bir ifadeyle CMK m. 134 hükmünün bu suç tipi açısından bir hukuka uygunluk nedeni olduğu belirtilmektedir. Ayrıca bu tür program ve cihazların kamu otoritesinin verdiği izne dayalı olarak bulundurulması ve imal edilmesinin hukuka uygun olduğu ifade edilmektedir[174].

---

170 Koca / Üzülmez, *Genel Hükümler*, s. 272.

171 Meşru savunma ve hakkın kullanılması hukuka uygunluk nedenlerinin bu suç tipi bakımından uyuşmadığı izahtan varestedir. Aynı yönde Akbulut, *Bilişim Alanında Suçlar,* s. 359.

172 Ünal, "Bilgisayarlarda, Bilgisayar Programlarında…", s. 115.

173 Akbulut, *Bilişim Alanında Suçlar*, s. 359; Özbek / Doğan / Bacaksız, s. 1027; Apaydın, s. 567.

174 Koca / Üzülmez, *Özel Hükümler*, s. 962.

Bir diğer görevin ifası bağlamında değerlendirilmesi gereken konu "**sızma testi**"dir. Kötü amaçlı bir saldırganın bilişim sistemlerine verebileceği zararları bildirmek ve bu zararları önleyebilecek ölçüde savunma tedbirlerini almak amacıyla bir kurumun bilişim sistemlerinde güvenlik zafiyetlerinin tespiti konusunda yetkili kılınmış kimseler tarafından uygulanan testlerin tümüne **sızma testi (penetration test)** adı verilmektedir[175]. "**Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik**"te[176] sızma testinin tanımı, m. 3, f. 1 ğğ bendinde, şu şekilde yapılmıştır:

> "*Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen güvenlik testlerini …ifade eder"*.

Sızma testi kapsamında bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları işlenebilmektedir. Burada yönetmelikte düzenlenen bir konunun, ilgili suç tipleri açısından hukuka uygunluk nedeni olup olmadığı hususunun değerlendirilmesi gerekir. Görevin ifasının kaynağını oluşturan kanun hükmünden anlaşılan şey sadece şekli anlamda kanun değildir, bilakis yazılı hukuk kurallarıdır. Dolayısıyla tüzük veya yönetmeliklerin de bu kapsamda olduğu belirtilmektedir[177]. Buradan hareketle sızma testlerinin uygulanmasının ve bu testleri uygulamak gayesiyle gerekli cihaz, program, şifre veya sair güvenlik kodlarının imal edilmesinin veya bulundurulmasının görevin ifası hukuka uygunluk nedeni dahilinde olduğu akla gelebilir. Madde gerekçesinde bu tür cihaz ve programların, bilişim güvenliğini test etmek amacıyla yapılmasının veya oluşturulmasının suç oluşturmayacağına vurgu yapılmaktadır. Fakat gerekçede bu durumun hukuka uygunluk nedeni kapsamında olup olmadığı belli değildir.

Günümüzde şirketler kurmuş oldukları bilişim sistemlerinin güvenliğini test etmek amacıyla bilişim güvenliği hizmeti sunan bir başka şirketten sızma testinin uygulanması bağlamında, sözleşme çerçevesinde hizmet alabilmektedirler. Bu noktada sızma testinin işlenen bilişim suçları bağlamında

---

[175] Ahu Karakurt Eren, "Sızma Testleri İle Türk Ceza Kanunu'nun 234, 244 ve 245/A Maddelerinde Düzenlenen Suçlar Arasındaki İlişkinin Değerlendirilmesi", *Terazi Hukuk Dergisi*, 15(164), 2020, s. 748; Bu test kapsamında risklerin, güvenlik açıklarının ortaya çıkarabileceği zararlar, saldırganların erişebileceklerin noktaların analizi yapılarak sistemler, bütüncül bir şekilde denetim altına alınır. Böylelikle zafiyetin tespitinden ziyade zafiyetin değerlendirilip sisteme erişim yollarının belirlenmesi ve yetkili erişim noktalarının kazanılması da bu testin hedefleri arasındadır. Bkz. Fatma Saliha Biter, *Siber Ansiklopedi*, s. 367.

[176] 15.03.2020 tarihli 31069 sayılı Resmi Gazete.

[177] Artuk / Gökcen / Alşahin / Çakır, s. 486; Koca / Üzülmez, *Genel Hükümler*, s. 276.

bir hukuka uygunluk nedeni oluşturduğuna işaret edilmektedir[178]. Her ne kadar bu testin uygulanmasının, ilgilinin rızası dahilinde bir hukuka uygunluk nedeni olarak görüldüğü ifade edilse de TCK m. 245/A hükmü çerçevesinde bunun, bir hukuka uygunluk nedeni olmadığı aşikardır[179]. Nitekim suçun mağdurunun toplumu oluşturan herkes olduğu ortadadır.

Kanaatimizce de CMK m. 134 hükmünün bu suç tipi bakımından bir hukuka uygunluk nedeni oluşturmadığını ifade etmek gerekir[180]. Buna sızma testlerini sağlayan cihaz, program, şifre veya sair güvenlik kodlarla ilgili seçimlik hareketlerinin hukuka uygun olduğu düşüncesi de eklenebilir. Zira bilişim alanında işlenen suçlar bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen başka bir suçun işlenebilme amacıyla hareket edilmediği ortadadır. Diğer bir anlatımla fiilin suç oluşturmaması bir hukuka uygunluk nedeninin varlığı ile ilgili olmayıp amaç unsurunun eksikliği dolayısıyladır[181].

[178] Bilişim sistemine girme suçu bakımından rızanın tipikliği ortadan kaldıran bir yönü vardır. Ancak veri nakillerini izleme suçu ve verileri yok etme veya değiştirme, erişilmez hale getirme, başka yere gönderme veya veri yerleştirme suçu açısından rızanın genel bir hukuka uygunluk nedeni olarak ele alındığı belirtilmektedir. Bkz. Karakurt Eren, "Sızma Testleri…", s. 753, 755, 756.

[179] Eisele, s. 928; Aynı yönde Akbulut, Bilişim Alanında Suçlar, s. 359; Karşı görüş için bkz. Korkmaz, s. 53; Kaya / Çakır, s. 48; Özel hüküm olan koruyucu programların etkisiz kılmaya yönelik hazırlık hareketleri suçunda (5846 s. K m. 72) ilgilinin rızasının hukuka uygunluk nedeni olduğu ifade edilse de bahse konu program veya teknik donanımların hangi koruyucu programı etkisiz kılacağı bilinmediği için hukuka uygunluk nedeni olan rızayı açıklamaya yetkili kişinin belirlenmesinin olanaklı olmadığından bahsedilmektedir. Bkz. Değirmenci, "Koruyucu Programlar…", s. 115, 116.

[180] Karakurt Eren, "Bilişim Alanında…", s. 238.

[181] Örneğin, 2937 sayılı Polis Vazife ve Salahiyet Kanunu Ek Madde 7, f. 1 hükmü uyarınca polis sanal ortamda istihbarat faaliyetlerinde bulunabilmektedir. Maddenin ikinci fıkrası uyarınca polis, ilk fıkrada belirtilen görevlerin yerine getirilmesine yönelik bilişim suçlarının işlenmesinin önlenmesi amacıyla hakim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürünün, Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanının veya bilişim suçlarıyla sınırlı olmak üzere bilişim suçları ile ilgili daire başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen verileri tespit edilebilir, dinleyebilir, sinyal bilgilerini değerlendirebilir ve kayda alabilir. Dolayısıyla bu işlemleri yapmaya yönelik bilgisayar programlarının bulundurulmasının suç oluşturmaması, bir hukuka uygunluk nedeninden ziyade, amaç unsurunun yokluğu yüzündendir.

D. Suçun Özel Görünüş Şekilleri

1. Suça Teşebbüs ve Etkin Pişmanlık Sorunu

Bulundurma/depolama gibi temadi özellikleri olan seçimlik hareketler hariç diğer seçimlik hareketler sırf hareket suçu niteliğini taşımaktadırlar[182]. Sırf hareket suçlarında ancak hareketin kısımlara bölünebildiği hallerde suça teşebbüsün mümkün olduğundan söz edilebilir. Örneğin, polisin müdahalesi sonucu suçun konusunu oluşturan cihazın satışı yarıda kalabilir. Fakat yukarıda da ifade edildiği üzere, satışa arz seçimlik hareketi gerçekleştiğinden fail, işlenen suçun cezasıyla cezalandırılır[183]. Öte yandan fail, bu nitelikteki bir programı internet üzerinden kendi bilgisayarına indirmeye çalışırken elektrik kesilebilir. Bu noktada "kabul etmek" seçimlik hareketi çerçevesinde teşebbüsten bahsedilebilir[184].

Temadi özelliği gösteren bulundurma/depolama seçimlik hareketlerinde fail, ilgili cihaz, program, şifre veya sair güvenlik kodlarını kendi egemenlik alanına geçirmesiyle suç tamamlanmış olur. Ancak failin elinde bulundurduğu/depoladığı süre dahilinde suç işlenmeye devam edecektir[185]. Bu çerçevede suça teşebbüs ancak ele geçirme anına kadar mümkündür.

Teşebbüsün mümkün olduğu durumlarda failin gönüllü vazgeçmeden de yararlanabileceği belirtilmektedir[186]. 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. Bu çerçevede bir sorun olmadığını düşünmekteyiz.

Failin suça ilişkin bir eylem planından yalnızca vazgeçmesi, başlangıçta yaratılan genel tehlikelilik boyutunu, geriye isnadı mümkün olmayan

---

182 Akbulut, *Bilişim Alanında Suçlar*, s. 359; Koca / Üzülmez, *Özel Hükümler*, s. 962; Dülger, s. 491.

183 Esasında bu seçimlik hareketin teşebbüs suçu olması sebebiyle teşebbüse elverişli olmadığı ifade edilmektedir. Bkz. Karakurt Eren, "Bilişim Alanında…", s. 240.

184 Madde hükmüyle hazırlık hareketlerinin cezalandırıldığından hareketle suçun, teşebbüse elverişli olmadığına vurgu yapılmaktadır. Bkz. Gül, s. 350; Her ne kadar soyut tehlike suçlarında hareketin kısımlara bölünebileceği ölçüde teşebbüsün mümkün olduğu belirtilse de cezanın belirlenmesi noktasında teşebbüs hükümlerinin nasıl uygulanacağının bir sorun oluşturduğuna işaret edilmelidir. Ünal, "Tehlike Suçları…", s. 337 vd.

185 Koca / Üzülmez, *Özel Hükümler*, s. 962.

186 Akbulut, *Bilişim Alanında Suçlar*, s. 359.

bir ölçüye indirgemeyecektir[187]. Çünkü hazırlık hareketlerine ilişkin suç tamamlanmıştır. Ancak hazırlık hareketlerinin işlenmesiyle birlikte buradaki tehlike kaynaklarının tehlikeye neden olma ihtimaline son verilebilmesi de mümkündür. Buradaki esas sorun **etkin pişmanlık** kurumu bakımından doğmaktadır. **TCK m. 245/A hükmünde failin etkin pişmanlıktan yararlanabileceğine dair bir düzenleme bulunmamaktadır**. Örneğin, failin kredi kartı kopyalama cihazlarını başkalarından almasına rağmen daha sonra pişmanlık duyarak adli makamlara sunmasının ceza hukuku sorumluluğunu doğurup doğurmadığını tartışmak gerekir. Bu doğrultuda öncelikle Al. CK §202c/2, §263a/4, §303a/3 ve §303b/5 hükümlerine bakılmalıdır. Bu hükümler Al. CK'nın §149 hükmünün 2. ve 3. paragraflarına atıf yapmaktadır. Bahse konu 2. paragraf, parada ve kıymetli damgada sahteciliğin hazırlık hareketlerinde gönüllü vazgeçmeyi ele alırken 3. paragraf ise etkin pişmanlık halini düzenlemektedir[188]. Etkin pişmanlık dahilinde fail, gerekli koşulları yerine getirirse tamamlanmış olan tehlike suçundan dolayı cezalandırılmayacaktır[189]. Buna benzer düzenleme TCK m. 201 hükmünde yer almaktadır. Maddenin ilk fıkrası, parada sahtecilik (TCK m. 197) ve kıymetli damgada sahtecilik (TCK m. 199) suçlarının etkin pişmanlık hallerini ele almaktadır. İkinci fıkrası ise TCK m. 200 hükmünde düzenlenen ve yukarıda kısmen değindiğimiz "**Para ve kıymetli damgaları yapmaya yarayan araçlar"** suçunun **etkin pişmanlık** halini düzenlemiştir[190]. Dolayısıyla fail,

---

[187] Sieber, s. 446.

[188] "Al. CK §149 2. paragraf ve 3. paragraf hükmü şu şekilde düzenlenmiştir:

"Her kim, gönüllü olarak,

1. hazırlanmış olan suçun icra hareketlerinden vazgeçer ve diğer kişilerin fiili hazırlamaya devam etmeleri ile veya suçu işlemeleri konusunda kendisi tarafından meydana getirilen tehlikeyi bertaraf eder veya fiilin tamamlanmasını engeller ve

2. halen mevcut bulundukları ve sahtecilik için kullanmaya elverişli oldukları takdirde, sahtecilikte kullanılan araçları imha eder, kullanılmaz hale getirir, bunların mevcudiyetini resmi bir makama ihbar eder veya bunları oraya teslim ederse,

Birinci fıkraya göre cezalandırılmaz

3. paragraf:

" Eğer, diğerlerinin fiili hazırlamaya devam etmeleri veya suçu işlemeleri tehlikesi, failin katkısı olmadan bertaraf edilmiş veya suçun tamamlanması engellenmiş ise, bu takdirde, ikinci fıkranın 1 numaralı bendindeki koşulların yerine, failin bu amaca ulaşmak için yaptığı gönüllü ve ciddi bir şekilde çaba göstermiş olması yeterlidir.", Bkz. Yenisey / Plagemann, s. 249, 250.

[189] Eisele, s. 928.

[190] TCK m. 201, f. 2 hükmü aynen şu şekildedir:

"*Sahte para veya kıymetli damga üretiminde kullanılan alet ve malzemeyi izinsiz olarak üreten,*

sahte para üretiminde kullanılan alet ve malzemeyi izinsiz bir şekilde ülkeye sokmuş ve daha sonra resmi makamlar haber almadan bu alet ve malzemenin ele geçirilmesini sağlamışsa hakkında cezaya hükmolunmayacaktır. Buna ilişkin hükmün TCK m. 245/A'da bulunmaması nedeniyle failin pişmanlık gösterip cihaz, program, şifre veya sair güvenlik kodlarının adli makamlarca ele geçirilmesini sağlasa dahi cezalandırılması ihtimali gündeme gelecektir. Bu noktada bu etkin pişmanlık hükmünün (TCK m. 201, f. 2) TCK m. 245/A hükmü kapsamında kıyasen uygulanıp uygulanmayacağı konusu akla gelmektedir. Ceza hukuku sisteminde kıyas kural olarak yasaksa da (TCK m. 2, f. 3) doktrinde ceza hukukunun genel hükümlerinde ceza sorumluluğunu sınırlandırıcı ölçüde kıyasın mümkün olduğu belirtilmektedir[191]. Buna karşılık etkin pişmanlığa ilişkin hüküm, genel bir hüküm değildir. Başka bir ifadeyle TCK m. 201'de yer alan hükümler yalnızca bahsi geçen ilgili suçlarla sınırlıdır. Dolayısıyla TCK m. 201, f. 2 hükmü kıyasa konu olmayacaktır. Bu noktada TCK m. 245, f. 5 hükmünde yer alan etkin pişmanlık hükmü de uygulama alanı bulamayacaktır. Zira madde hükmünün atıf yaptığı TCK m. 168 hükmünün kapsamı yalnızca malvarlığına karşı işlenen suçlarla sınırlıdır. Bu yüzden uygulamada doğabilecek tereddütlerin giderilmesi adına, TCK m. 201, f. 2 hükmüne benzer şekilde, TCK m. 245/A'ya özel bir etkin pişmanlık hükmü eklenmelidir.

2. İştirak

Madde hükmünde yer alan, satma ve satın alma, başkalarına verme ve kabul etme gibi seçimlik hareketler bakımından suçun çok failli bir suç özelliği gösterdiği söylenebilir[192]. Diğer bir anlatımla bu seçimlik hareketle sınırlı olarak suçun karşılaşma suçu olduğu ifade edilebilir. Bu durumda herkes faildir ve ceza hukuku sorumluluğu açısından istisnai hususlar söz konusu değildir. Bundan başka ilgili suç tipinde suça iştirak hükümleri açısından özel bir durum söz konusu olmayıp genel hükümlerin geçerli olacağı belirtilmelidir[193].

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."

191 Özgenç, s. 135; Aynı yönde Akbulut, *Genel Hükümler*, s. 87; Karşı görüş, Artuk / Gökcen / Alşahin / Çakır, s. 164; Koca / Üzülmez, *Genel Hükümler*, s. 66.

192 Koca / Üzülmez, *Özel Hükümler*, s. 960.

193 Akbulut, *Bilişim Alanında Suçlar*, s. 360; Özbek / Doğan / Bacaksız, s. 1028; Dülger, s. 491; Kusurluluğu ortadan kaldıran neden bağlamında failin cebir veya tehdit dolayısıyla irade

Örneğin, bilişim sistemine hukuka aykırı olarak giren bir programı imal eden kimse, daha sonra bu programı bir başka kişiye satabilir. Satın alan kimse daha sonra bu program sayesinde bilişim sistemine girme suçunu işleyebilir. Programı satan kişi, bilişim sistemine girme suçunun yardım edenidir. Fakat "failliğin **şerikliğe** nazaran önceliği" prensibi gereği programı satan kişi, yalnızca TCK m. 245/A hükmünden dolayı cezalandırılacaktır.

3. İçtima

Bu suç tipiyle işlenmesi amaçlanan suçların hazırlık hareketleri ceza hukuku sorumluluğu altına girmektedir. Dolayısıyla bu suç tipi bakımından araç suçu-amaç suçu ilişkisinden bahsetmek mümkündür. Bu suçun işlenmesi için amacın gerçekleşmesi gerekmez, bilakis bu amaçla ilgili seçimlik hareketlerin gerçekleştirilmesi yeterlidir. Ancak amaç suçun da ayrıca işlenmesi halinde gerçek içtima söz konusu olur. Bu bahisle örneğin; imal ettiği, satın aldığı, bulundurduğu bir cihaz veya programlarla bilişim sistemine girme suçunu işleyen fail gerçekleştirmiş olduğu her iki suçtan ayrı ayrı cezalandırılır[194].

Bu suç bakımından zincirleme suç (TCK m. 43, f. 1) hükümlerinin uygulanabilmesi için ilgili seçimlik hareketlerinin farklı zaman dilimlerinde gerçekleşmesi gerekmektedir. Aksi takdirde seçimlik hareketli suçların özelliği gereği ortada tek suç söz konusu olur[195].

Belirtilmelidir ki TCK m. 245/A hükmüyle özel kanunlarda bazı suç tiplerini düzenleyen hükümlerle bir görünüşte içtima hali olan genel norm-özel norm ilişkisi kurmak mümkündür. Bu bağlamda "**imza oluşturma, verilerin izinsiz kullanımı suçu"**na yer veren Elektronik İmza Kanununun 16. maddesi[196]; **"koruyucu programları etkisiz kılmaya yönelik hazırlık**

yeteneğinin etkilenmesi mümkündür. Bu bahisle doktrinde TCK m. 28 hükmünün TCK m. 245/A hükmünde yer alan suç açısından uygulanmasının mümkün olduğu vurgulanmaktadır. Buradan hareketle cebir veya tehdit uygulayan kişinin bu suçun işlenmesinde dolaylı fail olduğu noktasında herhangi bir kuşku bulunmamaktadır. İlgili açıklamalar için bkz. Karakurt Eren, "Bilişim Alanında…", s. 239, 241.

194 Koca / Üzülmez, *Özel Hükümler*, s. 962; Fidye virüsleriyle ilgili olarak hem bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçu (TCK m. 244, f. 2) hem de TCK m. 245/A suçu işlenmiş olur. Retornaz / Güçlütürk, s. 310. Bununla birlikte fidyenin temin edilmesi halinde bilişim sistemleri aracılığıyla haksız yarar sağlama suçunun (TCK m. 244, f. 4) da oluştuğu ifade edilmelidir.

195 Akbulut, *Bilişim Alanında Suçlar*, s. 361; Koca / Üzülmez, *Özel Hükümler*, s. 962; Özbek / Doğan / Bacaksız, s. 1028.

196 İlgili hüküm aynen şu şekildedir*:*

hareketleri suçu"nun yer aldığı Fikir ve Sanat Eserleri Kanunu'nun 72. maddesi[197] ve **"telsiz cihaz ve sistemlerinin izinsiz şekilde satma, işletme ve kullanma suçu"**nun **düzenlendiği Elektronik Haberleşme Kanunun 63. maddesinin 4. fıkrası**[198] özel hüküm olarak karşımıza çıkar[199]. Dolayısıyla özel hükümler kapsamına giren bir suç işlenmişse genel hüküm olan TCK'nın 245/A maddesi uygulanmayacaktır[200].

E. Yaptırım, Kovuşturma Usulü ve Uygulamadaki Durum

TCK m. 245/A maddesinde belirtilen suçun yaptırımı bakımından "*bir yıldan üç yıla kadar hapis ve beşbin **güne kadar adli para cezası***" öngörülmüştür. Öncelikle hazırlık hareketlerini cezalandıran bu soyut

---

*"Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; **imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar** ile **izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar** bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar.*

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."

197 İlgili hüküm aynen şu şekildedir:

"*Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla **oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran** kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır*."

198 İlgili hüküm aynen şu şekildedir:

"*Kurma ve kullanma izni ile ruhsatname alınması gereken telsiz cihazı veya sistemlerini bu Kanunun 37 nci maddesine aykırı olarak, Kurumdan izin almaksızın satan, kuran, işleten ve kullananlar hakkında ikibin güne kadar adlî para cezası uygulanır. Bu cihazları, gerekli izinler alınmış olsa bile millî güvenliği ihlal amacıyla kullananlar eylemleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde altı aydan bir yıla kadar hapis ve on bin güne kadar adli para cezası ile cezalandırılırlar."*

199 2918 sayılı Karayolları Trafik Kanununun 51. maddesinin 5. fıkrasında hız sınırlarının aşılıp aşılmadığını tespit eden cihazlarının tespit veya sürücüyü ikaz eden cihazların imal, ithali ve araçlarda bulundurulması fiillerine yaptırım olarak hafif hapis ve hafif para cezaları öngörülmüştür. Hafif hapis ve hafif para cezaları 5252 sayılı Kanunun 7. maddesi gereği idari para cezasına dönüştürülmüştür. Bu bakımdan kanunun m. 51, f. 5 hükmü bir suç değil, bir kabahattir. Bu yüzden kabahat teşkil eden bu fiili bir suç olarak gören görüşlerin hatalı olduğunu belirtmek gerekir. İlgili görüş için bkz. Kaya / Çakır, s. 51.

200 Koca / Üzülmez, *Özel Hükümler*, s. 963; Akbulut, *Bilişim Alanında Suçlar*, s. 361, Kaya / Çakır, s. 51; Yukarıda da ifade edildiği üzere, kredi kartlarının arkasında bulunan rakam ve harfler sair güvenlik kodları olarak kabul edilirler. Bu doğrultuda başkası tarafından üretilmiş sahte kredi kartını bu özelliğini satın alma veya kabul etme durumunda özel norm olan TCK m. 245, f. 2'deki suç işlenmiş olur. Dolayısıyla genel norm olan TCK m. 245/A hükmü, uygulama alanı bulamayacaktır. Bkz. Gül, s. 351.

tehlike suçunun ceza miktarını, işlenmesi amaçlanan diğer suçlarla birlikte değerlendirmek gerekir. Örneğin, nitelikli unsurlar ve netice sebebiyle ağırlaşmış haller haricinde bir soyut tehlike suçu olan bilişim sistemlerine girme suçuna (TCK m. 243, f. 1) kanun koyucu tarafından bir yıla kadar hapis veya adli para cezası takdir edilmiştir. Bu noktada bahse konu hazırlık hareketlerini suç haline getiren TCK m. 245/A hükmündeki ceza miktarının, TCK m. 244, f. 4'teki bilişim sistemi aracılığıyla haksız yarar sağlama suçu ve m. 245 hükmündeki banka veya kredi kartlarının kötüye kullanılması suçları hariç olmak üzere, diğer bilişim suçlarının ceza miktarıyla hemen hemen aynı ceza miktarlarına sahip olduğu görülmektedir[201]. Halbuki bu suçun haksızlık içeriğinin diğer bilişim suçlarına nazaran daha az olduğu aşikardır. **Nitekim yukarıda yer verdiğimiz 18. Uluslararası Ceza Hukuku Kongresi'nde de belirtildiği üzere, hazırlık hareketini cezalandıran suçtaki ceza miktarının, işlenmiş suç için öngörülenden daha hafif olması gerektiği vurgulanmıştır**. Böylelikle bu suç açısından hapis ve adli para cezası miktarının daha hafifletilmesi gerektiğini önermekteyiz[202,203]. Her ne kadar bu yaklaşıma iştirak etsek de bilişim alanında suç kapsamına alınan hazırlık hareketlerinin daha fazla cezalandırılması yönünde bir eğilimin

[201] Bununla birlikte bilişim sistemlerinin kullanılması suretiyle işlenen hırsızlık suçundaki (TCK m. 142, f. 2, bent e) ceza miktarının beş yıldan on yıla kadar hapis; nitelikli dolandırıcılık suçu (TCK m. 158, f. 1, bent f) açısından ceza miktarının üç yıldan on yıla kadar hapis cezası olduğu görülmektedir.

[202] Örneğin, Avusturya Ceza Kanunu'ndaki §126c hükmünde belirtilen ceza miktarı, 6 aya kadar hapis cezası ve 360 güne kadar adli para cezasıdır. Bu kapsamda diğer bilişim suçlarının ceza miktarlarına da bakılmalıdır. Kanunun §126a hükmünde yer alan verilere zarar verme (Datenbeschädigung) suçunun cezasının basit hali (§126a/1) 6 aya kadar hapis cezası ve 360 güne kadar adli para cezasıdır. Nitelikli unsurlar açısından; §126a/2 hükmü gereğince 2 yıla kadar, §126a/3 hükmü uyarınca 3 yıla kadar, §126a/4 hükmü bakımından 6 aydan 5 yıla kadar hapis cezası öngörülmüştür. Bilgisayar sisteminin işleyişini bozma suçunu (Störung der Funktionsfähigkeit eines Computersystems) düzenleyen §126b hükmüne göre suçun basit hali (§126b/1) 6 aya kadar hapis ve 360 güne kadar adli para cezasıdır. Nitelikli unsurlar açısından; §126b/2 hükmü gereğince 2 yıla kadar, §126b/3 hükmü uyarınca 3 yıla kadar, §126b/4 hükmü bakımından 6 aydan 5 yıla kadar hapis cezası öngörülmüştür.

[203] Benzer sorunun İngiltere'de yürürlükte bulunan Bilgisayarın Kötüye Kullanılması Kanunu'nda (Computer Misuse Act 1990) da mevcut olduğu ifade edilmektedir. Bilişim suçlarının hazırlık hareketlerini cezalandıran 3A maddesindeki ceza miktarı 12 aya kadar hapis cezasıdır. Bu ceza miktarının; amaç suçlar olan bilgisayara yetkisiz erişim (m. 1), başka bir suçu işlemek veya işlenmesini kolaylaştırmak için yetkisiz erişim (m. 2), kasten bilgisayarın işleyişine zarar verici yetkisiz hareketlerde bulunma (m. 3) ve ciddi zarar yaratan veya yaratma riski taşıyan hareketlerde bulunma (m. 3ZA) suçlarında öngörülen ceza miktarlarıyla hemen hemen aynı olduğu ve bu durumun da ilgili kriterle uyumluluğunun tartışmalı olduğuna işaret edilmektedir. İlgili açıklamalar için bkz. Tekin, s. 51.

olduğu belirtilmelidir[204]. Örneğin, Al. CK §202c hükmünde gerçekleştirilen 20.11.2015 tarihli Kanun değişikliği sonucunda hapis cezası, bir yıldan iki yıla çıkarılmıştır[205].

Adli para cezası bakımından alt sınır belirtilmemiştir. Fakat TCK m. 52 hükmü gereği alt sınırın 5 gün olduğu noktasında kuşku yoktur. Hapis cezasıyla birlikte adli para cezasına hükmedilmesi genel olarak ekonomik kazancın elde edildiği suçlarda başvurulan bir yöntemdir[206]. Suçun işlenmesi dolayısıyla bir gelir elde edildiği tespit edilmişse kazanç müsaderesinin uygulanması söz konusu olacak adli para cezası ise bahsi geçen alt sınır üzerinden belirlenecektir. Buna karşılık suçtan elde edilen gelirin tespit edilmesi mümkün değilse bu durumda hakim, adli para cezasını, alt sınır ile üst sınır arasında takdir edebilecektir[207].

Suçun işlenmesiyle tüzel kişinin yararına haksız bir menfaat sağlanabilir. Böylelikle TCK m. 246 hükmü uyarınca tüzel kişiye özgü güvenlik tedbirlerinin uygulanması gündeme gelir.

Suçun mağduru toplumu oluşturan herkes olduğundan soruşturulması ve kovuşturulması şikâyete bağlı değildir. Bu suç re'sen takip edilen suçlardandır[208]. 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 11. ve 12. maddeleri uyarınca görevli mahkeme, asliye ceza mahkemesidir. Bu kanunun m. 9, f. 4 hükmüyle özel kanunlarda başkaca hüküm bulunmadığı takdirde ihtisaslaşmanın sağlanması amacıyla, gelen işlerin yoğunluğu ve niteliği dikkate alınarak daireler arasındaki iş dağılımı, Hakimler ve Savcılar Yüksek Kurulu tarafından belirlenebilmektedir. Kurulun 25.11.2021 tarihli, 1229 sayılı Kararıyla ağır ceza ve asliye ceza mahkemelerinin bazı daireleri

---

[204] Cezaların asgari hadden verildiği noktasından hareket edilerek ceza miktarının artırılması gerektiği savunulmaktadır. Bkz. Apaydın, s. 570; Yaptırım miktarının yerinde olduğunu belirten görüş için bkz. Karakurt Eren, s. 244.

[205] İlgili hüküm, Yolsuzlukla Mücadele Kanunu (Gesetz zur Bekämpfung der Korruption) kapsamında değiştirilmiştir. Bkz. Bundesgesetzblatt, 20.11.2015, <https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s2025.pdf%27%5D__1636704254580>, Erişim Tarihi 12 Kasım 2021.

[206] Koca / Üzülmez, *Özel Hükümler*, s. 963.

[207] Akbulut, *Bilişim Alanında Suçlar*, s. 362.

[208] Özel hüküm kapsamındaki 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 72. maddesinde belirtilen suç ise şikayete bağlı bir suçtur.

bilişim suçlarına bakma yönünde ihtisaslaştırılmıştır[209]. 15.12.2021 tarihinden sonra bu suç bakımından kovuşturma, ihtisaslaştırılan daireler tarafından yürütülecektir.

Zaman bakımından uygulanma (TCK m. 7) kuralları gereği TCK m. 245/A hükmü ancak 07.04.2016 tarihinden sonra işlenen fiillere yönelik uygulanabilir. Başkaca bir suçu oluşturmadığı sürece, bu tarihten önce bilgisayar programının, şifrenin ve sair güvenlik koduyla ilgili maddede sayılan fiillerin işlenmesi, cezaya tabi değildir[210]. Yukarıda da açıklandığı bulundurma/depolama seçimlik hareketleri mütemadi suç özelliğini göstermektedir. Maddenin yürürlük tarihinden önce ilgili cihaz, program ve kodları bulunduran kimse, bu tarihten sonra da bulundurmaya devam ediyorsa bu suçu işlemiş olacaktır.

Yürürlük tarihi itibarıyla madde hükmünün mahkeme içtihatlarına yansıyan yönü az olmakla beraber yakın gelecekte daha fazla karşımıza çıkacağı aşikardır[211]. Bilindiği üzere ATM'lere yerleştirilen banka veya kredi kartı kopyalama cihazının yardımıyla başkalarına ait banka hesaplarıyla ilişkilendirilerek banka veya kredi kartının sahte olarak üretilmesi, TCK m. 245, f. 2 hükmünde yer alan suçu oluşturmaktadır[212]. Buna karşılık cihazların ATM'ye yerleştirilmesi dahi TCK m. 245, f. 2'deki suça teşebbüs kapsamında görülmemekte ve bir hazırlık hareketi olarak algılanmaktaydı. Bu durumda failin yalnızca TCK m. 136 hükmündeki kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçuna teşebbüsten dolayı cezai sorumluluğu gündeme

---

[209] 30.11.2021 tarih, RG: 31675, < https://www.resmigazete.gov.tr/eskiler/2021/11/20211130-2.pdf>, Erişim Tarihi 01 Aralık 2021.

[210] Akbulut, *Bilişim Alanında Suçlar*, s. 347.

[211] Özellikle kripto para borsaları bir program sayesinde kurulmaktadır. Bu program dolayısıyla bilişim sistemlerinin araç olarak kullanılması suretiyle nitelikli dolandırıcılık suçunun (TCK m. 158, f. 1, bent f) işlenmesi gayet kolaylaşmaktadır.

[212] *"Gerçek kartların manyetik şerit bilgilerini kopyalamak, şifrelerini elde etmek ve elde etmiş oldukları kart bilgilerini beyaz kart tabir edilen kartlar ile değişik amaçlarla ellerinde bulunan diğer kartlara encoder cihazı aracılığı ile kopyalayıp bankada bulunan hesaplarla ilişkilendirerek sahte kart üretme eyleminin kül halinde TCK.nun 245/2. maddesine uyduğu gözetilmeden, ayrıca TCK.nun 136. maddesiyle cezalandırılmasına karar verilmesi, …yasaya aykırı… CMUK 321. Maddesi uyarınca (BOZULMASINA)…"* Yargıtay 8. CD, 2016/6350 E, 2016/8725 K, 30.06.2016, <https://proxy.hacibayram.edu.tr:2089/belge/y-8-cd-e-2016-6350-k-2016-8725-t-30-06-2016/2445757/encoder>, Erişim Tarihi 22 Ekim 2021; Bir başka Yargıtay kararı için bkz. Yargıtay 8. CD, 2016/10088E., 2016/10339K., 10.11.2016, <https://proxy.hacibayram.edu.tr:2089/araama/mahkeme-kararlari>, Erişim Tarihi 22 Ekim 2021.

gelmekteydi[213]. Keza Yargıtay da bu yaklaşıma göre içtihat geliştirmişti[214]. Madde hükmünün yürürlüğe girmesinin akabinde bu tür fiiller dolayısıyla ceza hukuku sorumluluğu genişleyecektir. Yargıtay da bir kararında;

> "*Sanığın katılan bankanın ATM cihazına yerleştirdikleri düzenekle, işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmeye çalışmaktan ibaret eyleminde; bilişim sisteminin parçası olan ATM üzerinde gerçekleştirdiği hareketlerinin ayrıntılı olarak tespiti ve bu hareketin suça konu bankanın bilişim sisteminin bir parçası olan ATM'nin kısa süreli de olsa çalışmasına engel teşkil edip etmediği, bağlı bulunduğu bilişim sistemine (sistemin engellenmesi veya bozulması gibi) bir zarar verip vermediği hususları ilgili banka şubesinden sorulup, sanığın eyleminin "bilişim sistemini engelleme veya bozmak", "mala zarar (v)ermek" ve* ***07.04.2016 tarihli Resmi Gazetede yayınlanarak yürürlüğe giren 6698 sayılı Yasanın 30. maddesi ile TCK'ya eklenen 245/A maddesinin karşılaştırılması*** *ile sonucuna göre hüküm kurulması yerine uygulama yeri bulunmayan TCK.nun 245/2, 35. maddelerinden hüküm kurulması*"

şeklinde belirtmek suretiyle bu suç tipinin uygulanması gerektiğine vurgu yapmıştır[215]. Bunun sonucunda fail, gerçek içtima dolayısıyla hem

---

[213] **Gül, s. 348. Aynı yönde açıklamalar için bkz.** Aliusta / Benzer, s. 39; Apaydın, s. 570; Değişiklikten önce bu cihazların yalnızca bulundurulmasının cezalandırılmayan önceki hareket kapsamında olduğu belirtilmekteydi. Bkz. Tekin, s. 51.

[214] "*Sanığa yüklenen sahte kart üretme suçunda; sanığın, yanındaki kimliği tespit edilemeyen şahıs ile birlikte 07.08.2014 günü saat 16.26'da ING Bank'a ait ..... Apartmanı bahçesinde bulunan ATM'ye kart kopyalama aparatını yerleştirdiğinin, ATM den ele geçirilen kopyalama düzenekleri üzerinde ...Adli Bilişim Büro Amirliği tarafından yapılan inceleme neticesinde düzenlenen 04.09.2014 tarihli raporda; Toshiba marka 16 GB hafıza kartında 12 adet video dosyası ve 2 adet resim dosyasının tespit edildiği ve raporlanması için CD ye aktarılarak gönderildiğinin anlaşılması ve henüz kart üretildiğine veya üretilmeye teşebbüs edildiğine ilişkin dosyada delil bulunmaması karşısında; raporda bildirilen verilerin çözümünün yaptırılması, kişilere ait bilgilerin varlığının tespit edilmesi halinde sanığın eyleminin TCK.nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmek suçunu oluşturacağı, herhangi bir bilgi yok ise eylemin aynı suça teşebbüs suçunu oluşturacağı gözetilmeden, suç vasfında yanılgıya düşülerek yazılı şekilde TCK.nın 245/2. maddesi uyarınca hüküm kurulması*," Yargıtay 8. CD, 2018/1350E., 2019/13066K., 04.11.2019, <https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=-918#>, Erişim Tarihi 12 Ekim 2021; Konuyla ilgili bir başka karar için bkz. Yargıtay 8. CD, 2015/13192E., 2017/3451K. 26.04.2017, <https://proxy.hacibayram.edu.tr:2089/belge/y-12-cd-e-2015-13192-k-2017-3451-t-26-04-2017/2847175/ATM+kredi+kart%c4%b1+TCK+136>, Erişim Tarihi 12 Kasım 2021.

[215] Yargıtay 8. CD, 2016/3214E., 2016/10758K., 24.11.2016, <https://proxy.hacibayram.edu.

TCK m. 245/A hükmünden hem de TCK m. 136 hükmü uyarınca ayrı ayrı cezalandırılacaktır.

III. CİHAZIN, BİLGİSAYAR PROGRAMININ, ŞİFRENİN VEYA SAİR GÜVENLİK KODUNUN MÜSADERESİ SORUNU

TCK m. 245/A hükmünde belirtilen suçla ilgili olarak tartışılması gereken bir başka konu; suçun konusunu oluşturan cihaz, bilgisayar programı, şifre veya sair güvenlik kodlarının bir güvenlik tedbiri olan müsadereye tabi tutulmasıdır. TCK m. 54, f. 4 hükmünde belirtildiği üzere üretimi, bulundurulması, kullanılması, taşınması, alım ve satımı suç oluşturan eşya müsadere edilecektir. Hatta bu tür bir eşyanın suçta kullanılmasına veya suçun işlenmesine yönelik tahsis edilmesine gerek bulunmamaktadır. Eşyanın bulundurulması dahi suç oluşturduğundan, başka bir suçun işlenmesinde kullanılıp kullanılmadığının veya kime ait olduğunun, müsadere hükümlerinin uygulanmasında bir önemi bulunmamaktadır[216]. Kanaatimizce, eşyanın başlı başına bir tehlikeliliğinden bahsedilemez. Esasında buradaki tehlike, eşyanın niteliğini açıklamada kullanılan bir kavramdan ibarettir. Bu tür eşyaların niteliğinden hareketle kanun koyucu, bir tehlike kaynağı olduğuna dikkat çekerek bunlarla ilgili fiilleri suç haline getirmeye çalışmaktadır. Buradaki güvenlik tedbiri anlamındaki tehlikelilik, failin bu nitelikteki eşyaları kullanarak başka suçlar işleyebilme ihtimalini ifade eder. Bu niteliğe sahip eşya üzerinde müsadere uygulanarak, yani failin eşya ile olan bağlantısı sona erdirilerek bu tehlikelilik halinin önüne geçilmeye **çalışılır**[217]. Ezcümle TCK m. 245/A hükmünde yer alan cihazlar TCK m. 54, f. 4 hükmüne tabi eşya olup

tr:2089/belge/y-8-cd-e-2016-3214-k-2016-10758-t-24-11-2016/2660439/245_A>, Erişim Tarihi 11 Ekim 2021.

216 Mahmut Koca, "Türk Ceza Hukukunda Müsadere", (Lexpera Blog, 27 Mayıs 2020), <https://blog.lexpera.com.tr/turk-ceza-hukukunda-musadere/#fnref56>, Erişim Tarihi 26 Ekim 2021.

217 Ünal, "Tehlike Suçları…", s. 66, 86.

başka bir suç işlenmiş olmasa da müsadere edilecektir[218, 219].

Cihazların müsaderesi bakımından bir mesele ortaya çıkmasa da program, şifre veya sair güvenlik kodlarının müsaderesinin nasıl yapılacağı sorusu akla gelmektedir. Genellikle bu program, şifre veya güvenlik kodları, bir donanım veya cihaz üzerinden çalıştırılırlar. Bu noktada CMK m. 134 hükmüne bakmak gerekecektir. Nitekim madde hükmü müsadere konusuyla dolaylı olarak ilişki kurmaktadır. Madde hükmünde esas amaçlanan şey, cihaz veya donanımlara değil, bilakis verilere elkonulmasıdır. CMK m. 134, f. 2 hükmü bu bağlamda önemlidir. Buna göre, şifrenin çözümü yapılmış ve gerekli kopyalar alınmışsa elkonulan cihazlar gecikme olmaksızın iade edilecektir. İlaveten CMK m. 134, f. 4 hükmüyle de bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında veriler yedeklenirken bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmesi mümkün hale getirilmiştir. Buradan yola çıkılarak müsaderenin gerekli olduğu durumlarda ise TCK m. 54, f. 5 hükmünün uygulanması gerektiği doktrinde önerilmektedir[220]. Buna göre, bir şeyin sadece bazı kısımlarının müsaderesi söz konusu olursa, tümüne zarar verilmeden bu

---

218 Konuyla ilgili olarak verilen İstanbul Bölge Adliye Mahkemesi 17. Ceza Dairesi tarafından verilen karar da bu durumu ifade etmektedir:

"…her ne kadar sanığın TCK'nun 245/2. Maddesinden cezalandırılması istemi ile kamu davası açılmış ise de; aparatın ele geçirildiği yer ve içerisinde kopyalanmış veri olmaması nedeniyle söz konusu suçun icra hareketlerine başlamadığı anlaşıldığından atılı suçtan da cezalandırılamayacağı, sanığın eyleminin TCK'nun 245/A maddesinde düzenlenen yasak cihaz veya programlar bulundurma suçunu oluşturduğu ancak bu suçun yürürlülük tarihinin 07/04/2016 tarihi olduğu, suç tarihi itibariyle herhangi bir yaptırımının bulunmadığı anlaşılmakla, Beykoz 1. Asliye Ceza Mahkemesinin sanığın eylemine uygun olmayan bir şekilde vasıflandırmada hataya düşerek verdiği kararının kaldırılmasına ve sanığın atılı suçtan beraatine karar verilerek aşağıdaki gibi hüküm kurulmuştur…

…Her ne kadar sanığın eyleminin suç tarihinden sonra 07/04/2016 tarihinde TCK 245/a maddesi ile ihdas edilen suçu oluşturması ancak sanığın eylemini 29/11/2015 tarihinde gerçekleştirdiği suç tarihi itibariyle herhangi bir yaptırımın söz konusu olmaması ancak suç tarihinden sonra yürürlüğe giren anılan maddede eylemin suç olarak kabul edilmesi nedeniyle Beykoz Adli Emanetinin 2016/352 sırasında kayıtlı 1 adet ATM kopyalama cihazının TCK 54/1.maddesi gereğince MÜSADERESİNE…" Bkz. İstanbul Bölge Adliye Mahkemesi 17. CD, 2017/61E., 2017/575K. 05.04.2017, <https://www.lexpera.com.tr/ictihat/bolge-adliye-mahkemesi/istanbul-bam17-cd-e-2017-61-k-2017-575-t-5-4-2017>, Erişim Tarihi 27 Ekim 2021.

219 2918 sayılı Karayolları Trafik Kanununun m. 51, f. 5 hükmünde ise bu tür cihazların müsadere edileceği özel olarak belirtilmiştir. Fakat madde düzenlemesi bir kabahati öngördüğünden bu yaptırımı Kabahatler Kanunu m. 18'deki "mülkiyetin kamuya geçirilmesi" olarak anlamak gerekir.

220 Cumhur Şahin, "Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (CMK m. 134)", *Yaşar Hukuk Dergisi,* 1(2), 2019, s.278.

kısmı ayırmak mümkünse, yalnızca bu kısmın müsaderesine karar verilebilir. Örneğin, bilgisayardaki hard disk müsadere edilirken şüphelinin hard disk içindeki, suç teşkil etmeyen bilgilerin kopyasının kendisine iade edilmesi mümkün kılınmalıdır[221] . Buna karşılık 54, f. 4 hükmü karşısında uygulamanın bu yönde bir yaklaşım göstermediği ortadadır[222]. Kanaatimizce TCK m. 54, f. 5 hükmünü CMK m. 134, f. 4 hükmüyle birlikte değerlendirdiğimizde, elkonulan cihazların veya donanımların içindeki suçla ilişkili olmayan verilerin kopyasının teslim edilmesine imkan tanınmalıdır. Ancak program, şifre veya sair güvenlik kodunun bulunduğu elkonulan orijinal hard disk ve diğer donanımlar hakkında bu tedbire devam edilmeli ve TCK m. 54, f. 4 hükmü uyarınca müsaderesine hükmedilmelidir[223].

Belirtmek gerekir ki imal edilen program, şifre veya sair güvenlik kodları bulut bilişim üzerindeki bir verilerin erişilmesinde de kullanılabilir. Bunun için internete bağlanabilen alelade bir bilgisayarın varlığı yeterli olmakla beraber program, şifre veya sair güvenlik kodunun bilgisayarda bulunmasına dahi gerek yoktur. Bu durumda müsaderenin uygulanıp uygulanmayacağı sorunu baş göstermektedir. Kanaatimizce CMK m. 134 hükmü uygulandığında şüphelinin kullandığı bilgisayarda bu program, şifre veya sair güvenlik kodu tespit edilemediğinde elkonulan cihaz ve donanımlar, CMK m. 131 hükmü uyarınca şüpheliye iade edilmelidir[224]. Bulut bilişim üzerindeki verilerin erişilmesine özgülenen program, şifre veya sair güvenlik kodlarına yönelik **"saklanan bilgisayar verilerinin aranması ve bunlara elkonulması"** başlıklı AK-SSS m. 19, 3. paragrafta yer alan hüküm yol göstericidir. Buna göre, taraf devletlerden her biri, yetkili mercilerin kendi ulusal sınırları içinde; bir bilgisayar sistemine ya da bu sistemin bir parçasına veya bilgisayar verilerinin saklandığı cihazlara elkonulması ya da bunların benzer şekilde koruma altına alınması; bilgisayar verilerinin kopyalanıp alıkonulması, söz

---

221 Şahin, s. 279.

222 CMK m. 134, f. 4 hükmü uyarınca uygulamaya yansıyan durum için bkz. Dülger, s. 587 vd.

223 Nitekim bunların orijinallerinde her ne kadar silme işlemi gerçekleştirilse de başka bir program vasıtasıyla tekrar geri getirilebilmeleri mümkündür. Keza Yargıtay Ceza Genel Kurulu'nun bir kararında da bu husus şu şekilde yer almaktadır:

"*Olaydan sonra sanık ...'a ait Nokia E72 marka cep telefonuna ait hafıza kartındaki silinmiş görüntülerin* ***bilgisayar programı yardımı ile hafıza kartına geri yüklenmesi sonucunda*** *mağdure ve sanık ...'un anlatımına uygun bir şekilde cinsel ilişki sırasında çekilen fotoğraflar elde edilerek dosya içerisine alınmıştır*." YCGK, 2014/14-35e., 2016/49K. 09.02.2016, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=1905#, Erişim Tarihi 14 Kasım 2021.

224 Ünal, "Bilgisayarlarda, Bilgisayar Programlarında…", s. 128, 129.

konusu saklı bilgisayar verilerinin doğruluğunun muhafaza edilmesi; **erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez hale getirilmesi ya da silinmesi** ile ilgili olarak düzenleme yapmakla yükümlü kılınmışlardır[225]. Buradan hareketle bulut bilişim sistemine erişim sağlayabilecek programın, şifrenin veya sair güvenlik kodunun kullanılamaz hale getirilmesi yönünde bir düzenlemeye ihtiyaç vardır. Bu sayede yeni suçların işlenme ihtimalinin önüne geçilmektedir.

Söz konusu cihaz, bilgisayar programı, şifre veya sair güvenlik kodlarının, madde hükmünde belirtilen amaç doğrultusunda, bulundurulması dahi suç teşkil ettiği için bunların bulunmaması halinde kaim değerin müsaderesine (TCK m. 54, f. 2) ilişkin hüküm de uygulanmayacaktır[226]. Öte yandan fail, cihaz veya program satışından maddi menfaat elde etmiş olabilir. Bu durumda elde edilen maddi menfaat hakkında kazanç müsaderesi hükmü (TCK m. 55) uygulanabilecektir.

SONUÇ

Bilişim alanında işlenen suçlarla ve bilişim sistemlerinin araç olarak kullanılmasıyla işlenebilen diğer suçlarla mücadelenin etkinliğinin sağlanması amacıyla bu suçların hazırlık hareketlerinin cezalandırılmasına yönelik TCK m. 245/A hükmünde yer alan yasak cihaz veya programlar suçu düzenlenmiştir. Madde hükmü aynı zamanda cihaz, bilgisayar programı, şifre veya sair güvenlik kodları bakımından ortaya çıkan karaborsanın önlenmesine de hizmet edecektir.

Cezalandırılabilirlik alanının ön alana kaydırılması yukarıda zikredilen birtakım kriterlere **göre yürütülmelidir. Bu** kriterlere riayet edilmeksizin yapılan kanuni düzenleme, temel hak ve özgürlüklerin aşırı bir şekilde daralmasına yol açar. Bu noktada TCK m. 245/A hükmünü bu kriterlerle birlikte değerlendirmek gerekir. Öncelikle bu suçun, önemli hukuki değerlere yönelen ihlalin önlenmesi amacıyla ihdas edildiği görülmektedir. Özellikle "*bilişim sistemlerinin araç olarak kullanılması suretiyle"* işlenebilen

[225] Sözleşmenin açıklayıcı memorandumunun 199. paragrafında bu durum şu şekilde ifade edilmiştir:

"*Dolayısıyla verilere el koyma ya da onları benzer şekilde güven altına almanın iki işlevi vardır: 1) Örneğin verileri kopyalamak yoluyla delil toplamak, ya da 2) örneğin verileri kopyalamak ve daha sonra orijinal versiyonlarını erişilmez kılmak ya da taşımak yoluyla verileri müsadere etmek. El koymak, el konan verilerin nihai olarak silinmesi anlamına gelmemektedir."*

[226] Koca, Türk Ceza Hukukunda Müsadere.

diğer suçlar dikkate alındığında bu suç tipiyle birden fazla hukuki değerin korunduğu ortadadır. Bu yüzden bu suç tipinin ilgili kriterle uyumlu olduğunu ifade etmek mümkündür.

AK-SSS m. 6 hükmünde cihazların kötüye kullanılmasıyla ilgili suç ihdasına dair düzenleme yükümlülüğünün, TCK m. 245/A hükmü çerçevesinde, genel itibariyle karşılandığı sonucuna ulaşmaktayız. Hatta "*bilişim sistemlerinin araç olarak kullanılmasıyla işlenebilen diğer suçlar*" ifadesiyle bu hükmün daha geniş bir içeriğe sahip olduğundan bahsedilmelidir. Bu durum eleştiri konusu yapılmıştır. Keza hazırlık hareketleri suç haline getirilirken çok genel ve belirsiz ifadelere başvurulmaması gerekmektedir. Fakat hükmün geniş bir şekilde düzenlendiği ve kanunilik ilkesiyle bağdaşmadığı yönünde yapılan eleştirilere katılmamaktayız. Zira bilişim sistemlerinde yaşanan her bir gelişim sonucunda kanuni düzenlemeye başvurmak oldukça güçtür. Sözgelimi Al. CK §202c, §263/3a, §303a/3 ve 303b/3 hükümleri gibi ayrı ayrı düzenlemeler yerine tek bir hüküm koymak daha isabetli bir çözümdür. Buna karşılık madde hükmüyle madde başlığının birbirleriyle uyumsuz olduğu barizdir. Özellikle madde başlığındaki "yasak" ibaresinin yer almaması gerektiği düşüncesindeyiz. İlaveten madde başlığının suçun konusuna göre değil, fiile göre oluşturulması gerekmektedir. Bu yüzden madde başlığının "program ve cihazların kötüye kullanılması" şeklinde düzenlenmesi gerektiğini belirten öneriye katılmaktayız. Madde metni belirli olsa da formülasyonunun daha iyi yapılabileceği noktasında yapılan eleştirilere itibar etmekteyiz. Öncelikle hangi suçların işleneceğine ilişkin amaç unsuruna yer verilmelidir. Daha sonra suçun konularına yer verilerek seçimlik hareketler düzenlenmelidir. Bu açıdan yaklaşıldığında, yukarıda aynen yer verdiğimiz *Koca/**Üzülmez***'in önerdiği formülasyonun, isabetli olduğunu belirtmek gerekir.

TCK m. 245/A hükmünün, işlenmesi amaçlanan suçlarla bağlantılı bir şekilde kurgulandığı aşikardır. Bu bağlamda madde hükmünün, yukarıda bahsi geçen "s*uç haline getirilen fiillerin asıl suçun işlenmesine sıkı sıkıya bağlı olması"* kriterini karşıladığı düşüncesindeyiz. Belirtilmelidir ki bu durum kastın yanında amaç unsurunun varlığı ile mümkün olur. Böylelikle belirli bir zarar veya tehlikeye neden olma eğilimi içerdiği ifade edilerek hazırlık hareketini suç haline getiren ilgili düzenlemenin meşru olduğu sonucuna ulaşılır. Bu bakımdan TCK m. 245/A hükmünde amaç unsuruna yer verilmesini, olumlu olarak nitelendirmek mümkündür. Bu yolla soyut tehlike suçundaki cezalandırılabilirlik alanı da sınırlandırılmış olur. Özellikle "sızma testleri"ni uygulayabilecek kişilerin maddede belirtilen suçları işlemek amacı

dışında gerekli cihaz veya programları bulundurdukları açıktır. Bu durum aynı zamanda çift kullanımlı tehlike kaynaklarının yönetimi açısından da önemli olup sözleşmenin belirttiği esaslar dahilinde uyumludur.

Amaç unsuru bağlamında bu suçun yalnızca doğrudan kastla işlenebileceğini belirterek olası kast yönündeki görüşlere katılmamaktayız. Buna ek olarak sızma testi tanımına yer veren yönetmelik hükmü ile CMK m. 134 hükmünün TCK m. 245/A hükmü kapsamında bir suç oluşturmayacağı açıktır. Ancak suçun oluşmaması ilgili hükümlerin bir hukuka uygunluk nedeni olmasından değil, bilakis amaç unsurunun yokluğu yüzündendir. Ayrıca ilgilinin rızasının bu suç açısından bir hukuka uygunluk nedeni olduğu yönündeki görüşlere suçun mağdurunun toplumu oluşturan herkes olduğu gerekçesiyle itibar etmemekteyiz.

Yukarıda belirtilen bir diğer kritere göre, hazırlık hareketini cezalandıran suçtaki ceza miktarının, işlenmiş suç için öngörülenden daha hafif olması gerekmektedir. Halbuki TCK m. 245/A hükmündeki ceza miktarının TCK m. 244, f. 4 ve TCK m. 245 hükmünde yer alan suçlar hariç, hemen hemen aynı olduğu görülmektedir. Haksızlık içeriği de göz önüne alındığında bu suç tipi için öngörülen ceza miktarının fazla olduğu anlaşılmaktadır. Bu doğrultuda ceza miktarının azaltılması gerektiğini ifade etmekteyiz.

Parada sahtecilik ve kıymetli damgada sahtecilik suçlarının etkin pişmanlık hükümleri TCK m. 200'de yer almışken benzer şekilde TCK m. 245/A'da düzenlenen suç bakımından etkin pişmanlık hükmünün yer almaması bir eksiklik teşkil eder. Özellikle failin soruşturma aşamasından önce cihaz, bilgisayar programı, şifre veya sair güvenlik kodlarını adli makamlara teslimini sağlamasının bir ceza hukuku sorumluluğunu doğurmaması gerekir. Olması gereken açısından bu şekilde ifade edilse de TCK m. 200 hükmünün de genel bir hüküm olmaması sebebiyle kıyasen uygulanması mümkün değildir. Bu yüzden bu suç tipine özel olarak etkin pişmanlık hükmünün ihdasına ihtiyaç vardır. TCK m. 245/A hükmüyle ilgili etkin pişmanlık hükmünün ihdas edilmesi aynı zamanda bilişim alanında suçlar bakımından öne çıkan karaborsayla mücadelede önemli bir katkı sağlayacaktır. Zira bu hükümden yararlanmak isteyen kişiler bu karaborsanın izlenmesinde önemli bilgiler verebilirler. Böylelikle TCK m. 245/A'daki seçimlik hareketleri gerçekleştiren diğer kişilere de ulaşma imkanı yaratılmış olur.

Kural olarak bilişim alanında veya bilişim sistemlerinin araç olarak kullanılmasıyla işlenen suçların işlenmesi amacıyla tasarlanmış olan

cihazların TCK m. 54, f. 4 hükmü uyarınca müsaderesi yönünde bir sorun bulunmamaktadır. Zira üretimi, bulundurulması, kullanılması, taşınması, alım ve satımı suç oluşturan eşya müsadereye tabi olup bunların kullanılması suretiyle ayrı bir suç işlenmesi de gerekmeyecektir. Buradaki esas sorun bilgisayar programı, şifre veya sair güvenlik kodlarının müsaderesinin nasıl yapılacağına ilişkindir. Bu noktada hem CMK m. 134 hükmünün hem de TCK m. 54, f. 5 hükmünün de dikkate alınması gerekmektedir. Uygulama genellikle TCK m. 54, f. 4 hükmünü esas alsa da elkonulan cihaz veya donanımların içindeki suçla ilgili olmayan verilerin kopyasının teslim edilmesi gerektiği kanaatindeyiz. Bu yaklaşım hem koruma tedbirindeki hem de güvenlik tedbirindeki orantılılık ilkesiyle de uyumlu olur. Öte yandan bulut bilişim açısından bu sisteme erişimi mümkün kılan program, şifre veya sair güvenlik kodları hakkında AK-SSS m. 19, 3. paragrafındaki düzenlemeye göre hareket edilmesine ve bu yöne benzer ölçüde bir düzenleme yapılmasına ihtiyaç vardır.

Madde hükmünün yürürlüğe girmesiyle birlikte uygulamaya yansıyan kararların az oluşu dikkat çekmiştir. Yukarıda içtima başlığı altında zikrettiğimiz özel hükümlerin daha önce yürürlük kazandığı görülmekteyse de bunlar hakkında verilen yargı kararları da yok denecek kadar azdır[227]. Halbuki bilişim suçlarında Yargıtay kararlarının çoğunluğunun banka ve kredi kartlarının kötüye kullanılması suçu çerçevesinde olduğu düşünüldüğünde, TCK m. 245/A hükmünün uygulanması yönünde bir engelin olmadığı kanaatindeyiz. Özellikle HSYK'nın ilgili kararı doğrultusunda ihtisaslaştırılan mahkemeler aracılığıyla bu suç tipiyle ilgili olarak hükmedilen yargı kararlarının, daha da çeşitleneceğini öngörmekteyiz. Bu yönüyle HSYK'nın almış olduğu kararı olumlu olarak addetmekteyiz.

[227] Örneğin, Fikir ve Sanat Eserleri Kanununun m. 72 hükmündeki koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçunun, 71. maddede belirtilen manevi, mali veya bağlantılı haklara tecavüz suçuyla birlikte ele alındığı görülmektedir. Genellikle Yargıtay, bu yöndeki programların bulunduğunu işaret etse de kanunun 71. maddesindeki suçun oluşup oluşmadığını yönünde içtihatta bulunmaktadır. İlgili kararlarda 72. maddedeki suçunun oluşup oluşmadığı noktasında bir değerlendirmeye rastlanılmamaktadır. Ayrıntılı bilgi için, bkz. Değirmenci, "Koruyucu Programlar…", s. 115.

KAYNAKÇA

Akbaş H İ, "Tuş Kaydedici (Keylogger)", Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021.

Akbulut B, *Türk Ceza Hukuku: Genel Hükümler*, 4. Bası, Adalet Yayınevi, 2017.

Akbulut B, *Bilişim Alanında Suçlar*, 2. Baskı, Adalet Yayınevi, 2017.

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

Altuğ Ş, "Banka veya Kredi Kartlarının Kötüye Kullanılması", *Uyuşmazlık Mahkemesi Dergisi*, 9(17), 2021, s. 1-44.

Apaydın C, "Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu", *Terazi Hukuk Dergisi*, 15(163), 2020, s. 563-571.

Artuk M E / Gökcen A / Çakır K / İçer Z, *Türk Ceza Hukuku: Genel Hükümler*, 14. Baskı, Adalet Yayınevi, 2020.

Avrupa Konseyi Siber Suç Sözleşmesi, Açıklayıcı Memorandum, 2.7 paragraf, <https://rm.coe.int/16800cce5b#:~:text=The%20Convention%20and%20its%20Explanatory,II>, Erişim Tarihi 05 Ekim 2021.

Babayiğit B, "Deepfake'in Ceza Hukuku Bakımından Değerlendirilmesi Ve De Lege Ferenda Öneriler", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 25(4), 2021, s. 655-703.

Bilgiç A, "Kökset (Rootkit)", Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021.

Biter F S, "İstenmeyen Mesaj (Spam)", Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021.

Bostancı G E, "Arka Kapı", Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021.

Bozbayındır A E, "The Advent of Preventive Criminal Law: An Erosion of

The Traditional Criminal Law?", *Criminal Law Forum*, (29), 2018, s. 25-62.

Chart of signatures and ratifications of Treaty 185, Title: Convention on Cybercrime, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>, Erişim Tarihi 05 Ekim 2021.

Çalışkan S, "Ele Geçirme **(**Hijacking)", Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021.

Değirmenci O, "Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi", *Yaşar Hukuk Dergisi*, 1(2), 2019, s. 175-204.

Değirmenci O, "Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri Suçu", *Terazi Hukuk Dergisi*, 13(140), 2018, s. 112-117.

Dülger M V, *Bilişim Suçları ve İnternet İletişim Hukuku*, 8. Baskı, Seçkin Yayıncılık, 2020.

Eisele J, "Der Kernbereich des Computerstrafrechts", *JURA*, Heft 12, 2021, s. 922-934.

Erdem M / Özocak G, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 69(1), 2019, s. 127-212.

Eren Karakurt A, "Sızma Testleri İle Türk Ceza Kanunu'nun 234, 244 ve 245/A Maddelerinde Düzenlenen Suçlar Arasındaki İlişkinin Değerlendirilmesi", *Terazi Hukuk Dergisi* 15(164), 2020, s. 747-764.

Eren Karakurt A, "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*, 11(43), 2020, s. 212-246.

Erken E, "Truva Atı", Naci Akdemir / Can Ozan Tuncer (Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021.

Eroğlu C, "Stuxnet Solucanı Saldırısı-2010", Naci Akdemir / Can Ozan Tuncer

(Ed.), *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım*, Pegem Akademi, 2021.

Gül A, *Doğrudan-Dolaylı Bilişim Suçları*, 3. Baskı, Seçkin Yayıncılık, 2021.

Heger M, "§ 202c", Karl Lackner / Kristian Kühl (Ed.), *Strafgesetzbuch-Kommentar*, 29. Auflage, C.H Beck, 2018.

Kaya İ S / Çakır A, "Yasak Cihaz veya Programlar Suçu", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi,* (38), 2020, s. 32-55.

Koca M / Üzülmez İ, *Türk Ceza Hukuku: Genel Hükümler*, 14. Bası, Seçkin Yayıncılık, 2021.

Koca M / Üzülmez İ, *Türk Ceza Hukuku: Özel Hükümler*, 7. Baskı, Adalet Yayınevi, 2020.

Koca M, "Türk Ceza Hukukunda Müsadere", (Lexpera Blog, 27 Mayıs 2020), <https://blog.lexpera.com.tr/turk-ceza-hukukunda-musadere/#fnref56>, Erişim Tarihi 26 Ekim 2021.

Korkmaz İ, "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarını İşlemek Amacıyla İmal ve Ticareti Suçu", *Terazi Hukuk Dergisi*, 13(142), 2018, s. 47-55.

Nestler N, "Hacker-Tools im StGB", *Juristische Ausbildung,* 6, 2021, s. 629-637.

Önok M, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Prof. Dr. Nur Centel'e Armağan*, 19(2), 2013, s. 1229-1270.

Özbek V Ö / Doğan K / Bacaksız P, *Türk Ceza Hukuku: Özel Hükümler*, 16. Baskı, Seçkin Yayıncılık, 2021.

Özgenç İ, *Türk Ceza Hukuku: Genel Hükümler*, 17. Bası, Seçkin Yayıncılık, 2021.

Puschke J, "Grund und Grenzen des Gefährdungsstrafrechts am Beispiel der Vorbereitungsdelikte", Roland Hefendehl (Ed.), *Grenzenlose Vorverlagerung des Strafrechts?*, Berliner Wissenschafts Verlag, 2010, s. 9-40.

Pütz W, "Der Gefahrbegriff im Strafrecht", Universität Köln, *Dissertation*, 1936.

Reitinger P R, "Encryption, Anonymity and Markets", Douglas Thomas/ Brian D. Loader (Ed.), *Cybercrime: Law Enforcement, Security And Surveillance In The Information Age, Routledge*, 2003.

Retornaz E A / Güçlütürk O G, *Gelişen Teknolojiler ve Hukuk*, Oniki Levha Yayıncılık, 2020.

Sieber U, *Bilişim Teknolojisi İle Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku*, Feridun Yenisey, Salih Oktar, Zehra Başer Doğan (Çev.), Seçkin Yayıncılık, 2021.

Tekin D, "Bir Ceza Politikası Olarak Hazırlık Hareketlerinin Cezalandırılması: Türk ve İngiliz Yasal Düzenlemelerin Karşılaştırmalı Analizi", *Terazi Hukuk Dergisi*, 13(147), 2018, s. 49-60.

Türk Ceza Hukuku Derneği, 18. Uluslararası Ceza Hukuku Kongresi, Hazırlık Hareketleri ve İştirakin Genişlemesi, <https://www.tchd.org.tr/18-uluslararasi-ceza-hukuku-kongresi/#1541890191101-bb047707-5831>, Erişim Tarihi 27 Eylül 2021.

Turan M, *Bilişim Hukuku*, 5. Baskı, Seçkin Yayıncılık, 2021.

Ünal O G, Türk Ceza Hukukunda Tehlike Suçları, *Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Yayımlanmamış Doktora Tezi*, 2020.

Ünal O G, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma", *Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi*, 2011.

Yenisey F / Plagemann G, *Alman Ceza Kanunu, Strafgesetzbuch*, 2. Baskı, Beta Yayınevi, 2015.

Weber U, "Die Vorverlagerung des Strafrechtschutzes durch Gefährdungs und Unternehmensdelikte", *Beiheft zur Zeitschrift für die gesamte Strafrechtwissenschaft*, Walter de Gruyter, 1987.