Araştırma Makalesi

YASAK CİHAZ VEYA PROGRAMLAR SUÇU

İslam Safa KAYA[*] / Adem ÇAKIR[**]
ORCID: 0000-0001-5681-0756 / ORCID: 0000-0002-7082-3825

ÖZ

Teknolojinin ilerlemesi ve internet vasıtasıyla veri barındıran, işleyen ve paylaşan ürünlerin (bilişim) gündelik hayatta daha fazla yer edinmesi devletleri bu sahada hukuki altyapı hazırlamaya mecbur kılmıştır. Çünkü bu ürünlerin kötü niyetli kişilerce ele geçirilmesi telafi güç zararların doğmasına neden olacaktır. Avrupa Konseyi Siber Suç Sözleşmesi (2001) uluslararası alanda akdedilmiş çok önemli bir sözleşmedir. Bu sözleşme ile üye devletler, bilişim alanında işlenen suçlarla mücadele etmek amacıyla ulusal mevzuatlarını yakınlaştırma ve bazı suçları kanunlaştırma gibi taahhütlerde bulunmaktadır. Türkiye mezkûr sözleşmeyi 2010 yılında imzalamış ve 2014 yılında Sanal Ortamda İşlenen Suçlar Sözleşmesi adıyla yürürlüğe sokmuştur. Sözleşmenin gereği olarak birtakım değişiklikleri iç hukukuna yansıtmıştır. Bahsi geçen değişikliklerden bir tanesi de TCK 245/A olarak düzenlenmiş yasal cihaz veya programlar suçudur. Yasak cihaz veya programlar suçu sistematik açıdan, doğal olarak, bilişim alanında suçlar bölümüne eklenmiştir. Madde kendisine kaynaklık eden sözleşme madde 6 ile genel olarak, uyumludur. Öğretide maddenin başlığı ve içyapısı (anlaşılmaktan uzak olması) sıkça eleştirilmektedir. Yasak cihaz veya programlar suçu birçok yönü ile incelemeye değerdir. İlk olarak, bağımsız bir madde ile düzenlenmiş en yeni suçlardan biridir. İkincisi, Türk ceza hukukunda yer alan hazırlık işlemlerinin doğrudan cezalandırılmaması ilkesine aykırılık teşkil etmesidir. Gerçekten bu madde sayesinde bazı suçları işlemek için harekete geçilmesi bağımsız bir suç haline getirilmiş ve böylelikle bu suçların hazırlık işlemleri cezalandırılabilecektir. Son olarak, suç kapsamının geniş tutulmasının pratikte bir sıkıntıya sebebiyet verip vermeyeceği henüz tecrübe edilmemiştir. Bu bağlamda yargının vereceği kararlar oldukça önemli olacaktır.

Anahtar Kelimeler: Avrupa Konseyi Siber Suç Sözleşmesi, Sanal Ortamda İşlenen Suçlar Sözleşmesi, Bilişim Suçları, Yasak Cihaz, Yasak Program

Research Article

PROHIBITED DEVICE OR PROGRAMS

ABSTRACT

Following the mass advances in technology and with the help of the internet, devices that process, involve, and share information (i.e. informatics) have taken much more places in our daily lives. As a result of this, states have been obliged to build legal infrastructures; considering the very likelihood for such devices to be captured by individuals with bad intentions, which would result in some unrepairable damages. The Council of European Convention on Cybercrime (2001) is an essential covenant that has been signed on international level. Member states, under the responsibility that this act brings with it, have promised to re-organize their national criminal codes similarly in the fight against cybercrimes and to legislate certain cybercrimes. Turkey signed the above-mentioned convention in 2010 and ratified it in 2014. In accordance to the covenant, Turkey has adopted various changes to its national legal system. One of the reforms that have been brought into the legal system is TCK (Turkish Criminal Code) 245/A, also known as Article 245/A - Prohibited Devices and Programs. Prohibited Devices and Programs Article has systematically been, by its nature, categorised under the topic of cybercrimes. This article is, generally speaking, parallel to the Article 6 of the Convention. In the literature, the title, and the content (its ambiguity) of the article is oftentimes criticised. Prohibited Devices and Programs crime is worth analysing from a number of perspectives. Firstly, it is one of the newest crimes that are regulated under a separate Article. Secondly, it differentiates from one of the very fundamental principles in the Turkish Criminal Code that signifies "preparations to a crime cannot be punished." With the help of this Article, some preparations to crimes were identified as non-dependant crimes, and in this way, preparation steps to crimes may, currently, be punished. Lastly, whether the fact that crime's range is too wide is going to cause various problems or not has not yet been experienced. From this perspective, decisions given by the Turkish courts are going to be significant.

Keywords: The Council of European Convention on Cybercrime, Convention on Cybercrimes Committed Via the Internet, Informatics Crimes, Prohibited Device, Prohibited Program

[*] *Doç. Dr., Kırıkkale Üniversitesi Hukuk Fakültesi Milletlerarası Hukuk ABD Öğretim Üyesi, islamsafakaya_6@hotmail.com;* *Makale Geliş Tarihi/Received: 13.07.2020, Makale Kabul Tarihi/Accepted: 30.09.2020.*
[**] *Arş. Gör., Kırıkkale Üniversitesi Hukuk Fakültesi Hukuk Tarihi ABD Öğretim Görevlisi, ademcakir-1907@hotmail.com.*

GİRİŞ

Bilgisayar başta olmak üzere elektronik cihazların ve internetin yaygınlaşması gündelik hayatta kolaylık sağlamakla birlikte insanların kişisel ve malvarlığına ilişkin bilgilerini 3. kişilerin erişimine de müsait hale getirmiştir. Bu bakımdan yüzyıllarca bilinen suç tiplerine yenileri eklenmek zorunda kalınmıştır.

Öğretideki çeşitli kavram kullanımlarına girmeksizin,[1] bilişim kavramının bilgisayardan daha geniş (post cihazı, ATM, modem gibi) bir kullanıma karşılık geldiği ifade edilmelidir.[2] Bu yüzden TCK'de bilgisayar suçları yerine bilişim suçları şeklinde bir başlık kullanılmasının isabetli olduğu kabul edilmelidir[3]. Ayrıca bilişim alanının kapsamı belli bir sınırlanmaya tabi olamayacak kadar geniştir[4]. Teknolojinin gelişmesiyle birlikte kapsam genişlemeye devam edecektir[5]. Gelişmelerle birlikte fiziki olan her şey sanal ortama taşınmaya başlamış, bunun yanında bilişim odaklı saldırılar artmıştır[6]. Hukukun bu gelişme hızına yetişmesi ve hukuki koruma sağlaması güçleşmektedir[7].

Bilişim sistemlerinin bankacılık başta olmak üzere ekonomik düzeni idare etmesi ve kişisel verileri saklaması nedeniyle herkesi etkilemesinden ötürü bilişim suçları[8], topluma karşı işlenen suçlar kısmında yer almaktadır[9]. TCK'de ayrı bir başlık olarak tanzim edilen bilişim alanında suçlar bölümünün tüm bilişim suçlarını içerdiğini söylemek doğru olmaz[10]. Gerçekten klasik suç olarak sayılabilecek birçok suç, bilişim sistemlerinin kullanılmasıyla da işlenebilmektedir[11].

TCK ilk kabul edildiğinde bilişim alanında suçlar bölümünde 4 maddede toplam 10 fıkra bulunmakta idi. Zaman içerisinde yapılan ilavelerle bölüm, 5 madde ve 15 fıkraya erişmiştir. Ayrıca bazı maddelere yeni detaylar kazandırılmıştır. Bölüme 07.04.2016'da Resmi Gazete'de yayımlanarak eklenen tek madde, konumuz olan ''245/A Yasak cihaz veya programlar'' suçudur.

Çalışmamız iki ana temelde yükselecektir. İlk bölümde, yasak cihaz veya programlar suçu ile ilgili temel bilgiler vereceğiz. Budapeşte'de 2001 tarihinde

---

[1] Bilişim ifadesi yerine kullanılan kavramlarla ilgili 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)*,Cilt 19, Sayı 2, 2013, s. 1230-1231.

[2] Murat Volkan DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, 7. Baskı, Seçkin, Ankara, 2018,s. 69. Yazar, bu kıyaslamanın yanlış olduğunu zira bilişimin bir bilim alanı bilgisayarın bir makine olduğunu ancak olası bir karışıklığın önüne geçmek adına kıyaslamanın önemli olduğunu vurgulamaktadır.

[3]Ali İhsan ERDAĞ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", *Gazi Üniversitesi Hukuk Fakültesi Dergisi* Cilt: XIV, Sayı: 2,2010, s. 279.

[4] Alaattin BÜK, *Bilişim Alanında Kişisel Verilerin Korunması*, Seçkin, Ankara, 2018, s. 51.

[5]Tunç DEMİRCAN, *Bilişim Alanında Suçlar,* Legal Yayıncılık, İstanbul, 2016, s. 22.

[6]Salim KURNAZ & S. Mustafa ÖNEN, "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri", *International Journal of Politicsand Security*, Cilt 1, Sayı 2, 2019, s. 83.

[7] Yavuz ERDOĞAN, *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargı Kararları İle)*, Legal Yayıncılık, İstanbul, 2013, s. 43-44.

[8] Öğretide isimlendirme hususunda birlik yoktur. Ayrıntı için bkz. Hüseyin AKARSLAN, *Bilişim Suçları*, 2. Baskı, Seçkin, Ankara, 2015,s. 35-36.

[9] Mahmut KOCA & İlhan ÜZÜLMEZ, *Türk Ceza Hukuku Özel Hükümler*, 6. Baskı, Adalet Yayınevi, Ankara, 2019, s. 843.

[10] Ahmet GÜL, *Doğrudan/Dolaylı Bilişim Suçları*, 2. Baskı, Seçkin, Ankara, 2018,s. 25.

[11] Ulusal ve uluslararası bilişim mevzuat için bkz. Murat Volkan DÜLGER, *Bilişim, Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı*, 5. Baskı Seçkin, Ankara, 2019, s.29-458.

imzalan Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS)[12], öncesinde var olan birçok anlaşma ışığında bilişim alanında işlenebilecek suçlarla mücadeleyi uluslararası seviyede mümkün kılmaktadır. Türkiye Cumhuriyeti ilgili sözleşmeyi imzalamış[13] ve bu çerçevede değişiklikler yapmıştır[14]. Yasak cihaz veya programlar suçu bu sözleşmeye uyum sağlamak adına düzenlenmiştir. Madde ile ilgili eleştiriler göze çarpmaktadır.

İkinci bölümde yasak cihaz veya programlar suçunu temel bilgiler çerçevesinde inceleyeceğiz. Korunan hukuki değer, suçun unsurları, suç soruşturulması ve kovuşturulması özel görünüş biçimleri ve suçla ilgili diğer kanunlardaki düzenlemelere yer vereceğiz.

I. GENEL OLARAK

Yasak cihaz veya programlar suçunun arka planında 2001 tarihli Avrupa Konseyi Siber Suçlar Sözleşmesi vardır. Sözleşme, internetin gelişimiyle ortaya çıkan yargısal sorunları çözmek amacıyla yaratılmıştır. Sözleşmenin sunduğu çözüm, siber suç kanunlarını uyumlaştırmak ve siber suç davalarının etkinliğine yardım edecek mekanizmaların varlığını garanti altına almaktır.

Yasak cihaz veya programlar suçu, yukarıda da ifade edildiği gibi Türk Ceza Kanunu'na 2016 yılında giren bir suçtur. Kanuna yeni numaralı bir madde eklemek yerine bilişim alanında suçlar bölümünde 245. maddenin devamına 245/A maddesi olarak eklenmiştir. Aslına bakılırsa bu sözleşmeye uyum sağlamak için başka değişiklikler de yapılmıştır. Ancak 245/A bağlamında incelenmesi gereken temel madde, sözleşmenin 6. maddesidir.

A. SANAL ORTAMDA İŞLENEN SUÇLAR SÖZLEŞMESİ

Bilişim suçlarının dünya genelinde yaygınlaşmasıyla birlikte birçok devlet bu suçla mücadele edebilmek için ülke içi yasal düzenlemelerin uyumlaştırılması (harmonisation) gerekliliğinin farkına varmış; birçok uluslararası kuruluş da karar ve prensipler yayınlamıştır. Avrupa Konseyi, 1985 yılında başladığı çalışmalarını 2001 yılında Budapeşte'de Sanal Ortamda İşlenen Suçlar Sözleşmesi'ni[15] imzaya açarak nihayete erdirmiş ve tüm devletler için örnek bir sözleşme ortaya koymuştur.

Uyumlaştırma alelade bir hedef olmayıp, bu çalışma ile bilişim suçu işlemeyi düşünen kişilerin kendilerine güvenli liman (safe havens) olabilecek ülkeleri bularak suç işleme fırsatı yakalamalarının önüne geçmek amaçlanmıştır[16]. Uyumlaştırma çabalarının güçlüğüne[17] ve Çin ve Rusya[18] gibi önemli ülkelerin imzalamamasına

[12] Convention on Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 E.T: 04.04.2020.

[13] Türk kanun koyucu "Sanal Ortamda İşlenen Suçlar Sözleşmesi" ismiyle kanunlaştırılmıştır. https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf E.T: 04.04.2020.

[14] Türkiye'nin ilgili sözleşmeyi imzalama süreci için bkz. Cahit ALİUSTA & Recep BENZER, "Avrupa Siber Suçlar Sözleşmesi Ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2018, Cilt:4, No: 2, s. 35-42.

[15] Bu aşamadan itibaren "Sözleşme" olarak anılacaktır.

[16] Jonathan CLOUGH, "A World Of Difference: The Budapest Conventıon On Cybercrıme And The Challenges Of Harmonisation", *Monash University Law Review* (Vol 40, No 3), 2014, s. 701.

[17] Sözleşmenin uyumlaştırma sürecinde maruz kaldığı zorluklar için bkz. CLOUGH, 2014, s. 701 vd.

[18] Sözleşmeyi imzalamayan bazı ülkelerin çekinceleri/ileri sürdükleriyle ilgili bkz. Keir GİLES, *Prospects For The Rule Of Law In Cyberspace*, Strategic Studies Institute and U.S. Army War College Press, 2017, s. 22 vd.

rağmen Sözleşme, taraf olmayan birçok devleti de etkilemiş[19] ve bilişim suçlarıyla ilgili en kalıcı ve en geniş çapta imzalanmış çok uluslu anlaşma vasfına sahip olmuştur[20].

Sözleşmede işaret edilen temel suç kategorileri; bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar (m. 2-6), bilgisayarla bağlantılı suçlar (m. 7-8), içerikle bağlantılı suçlar (m. 9), telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar (m. 10) şeklindedir. Sözleşmede daha çok tercih edilen isim bilgisayar suçu ifadesidir. Buradan hareketle; bilgisayar; a) doğrudan suçtan etkilenen bir sistem, b) belli suçları işlerken kullanılan bir araç ve c) barındırdığı verilerin suç konusu olduğu veri kaynağı şeklinde tarif edilebilir. Yani bilgisayar/bilişim hem hedef suç hem araç suç olabilecektir[21].

Sözleşmenin amaçladığı ve sağladığı en önemli husus, bilgisayarla işlenen veya bilgisayarla ilişkili suçların belirlenip düzenlenmesinde ortak asgari standart getirmiş olmasıdır.

TCK 245/A için mehaz kabul edilen sözleşmenin 6. maddesi şu şekildedir;

"*Madde 6 - Cihazların kötüye kullanımı*"

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

[19]Emilio C. VİANO "Cybercrime: Definition, Typology, and Criminalization", *Cybercrime, Organized Crime and Societal Responses, International Approaches (Ed. Emilio C. Viano),* Springer Nature, Cham, Switzerland 2017, s. 15.

[20]Michael A. Vatis, "The Council of Europe Convention on Cybercrime", *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, 2010, s. 219-220.

[21]Serkan GÖNEN & Halil İbrahim ULUS & Ercan Nurcan YILMAZ, "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme", *Bilişim Teknolojileri Dergisi*, Cilt: 9, Sayı: 3, 2016, s. 230.

getirilmesiyle alakalı olmaması kaydıyla, işbu maddenin 1. paragrafını uygulamama hakkını saklı tutabilir."

Cihazların kötüye kullanımı başlıklı 6. maddesi uyarınca; sözleşmenin madde 2- yasadışı erişim, madde 3- yasadışı araya girme, madde 4- verilere müdahale, madde 5- sisteme müdahale başlıklı suçlarını işlemek için bir bilgisayar programı da dâhil olmak üzere cihaz, bilgisayar şifresi, erişim kodu veya benzer bir veri tasarlamak veya üretmek üye devletlerce suç kabul edilecektir. Taraf devletler bu hususta yasal düzenlemeleri yapacaktır. Bu sayede bu suçlar, kaynağında cezalandırılabilir hale getirilmektedir.

Maddede öne çıkan ilk unsur; cezalandırma için eylemin kasıtlı (intentionally) ve haksız bir şekilde (without right) yapılmış olması gerekliliğidir. Bu iki şartın doğal sonucu, bir eylemin cezaya konu olabilmesi için failin kastı özel olarak aranmalı ve ispat edilmelidir. Kasıt, diğer bir açıdan, özellikle doğası gereği çift kullanım "dual-use"[22] özelliğine sahip cihazların kullanımında yasal veya gayri yasal ayrımı için de belirleyici bir unsurdur[23].

Fıkra 1- a "*üretimi, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı veya başka şekilde erişilebilir hale getirilmesi*" diyerek hangi eylemlerin suç sayılabileceğini göstermektedir. i) bendinde, bilgisayar programı da dahil olmak üzere cihaz ifadesi kullanılmıştır. Açıklayıcı raporda bilgisayar sistemi hem hardware hem software içeren bir cihaz olarak açıklanmıştır[24]. Bu yüzden, cihazın software fonksiyona sahip bir anlamı olduğu kabul edilmelidir[25]. ii) bendinde bilgisayar şifresi, erişim kodu ve benzeri veriler ifadesi geçmektedir. Bunlar bir bilgisayar sisteminin tamamına veya bir kısmına erişmeyi mümkün kılmaktadırlar[26].

Fıkra 1-b "*Taraflardan biri, yasa gereği cezaî sorumluluğun doğması için bahsi geçen öğelerden belli bir sayıda bulundurulmasını şart koşabilir*." Buna göre, suçun doğması bakımından bulundurma fiilinin gerçekleşmesi için taraf devletler öğelere (item) bir sayı sınırı şart koşulabilir. 2003 tarihinde ABD Senatosuna başkanlıktan tarafından AKSSS ile ilgili sunumda bu bent ile ilgili sayının (18 U.S. Code § 1029(3) göre dolandırıcılık amacıyla 15 ve üzeri cihaz bulundurulması gerekir)[27] 15 ve üzeri olarak yürürlüğe sokulması tavsiye edilmiştir[28].

Maddenin 2. fıkrasında açıkça 2 ila 5. maddelerde sayılan suçları işlemek amacı gütmeyen bir fiilin cezalandırılamayacağı yazılıdır. Bu husus bir bilgisayar sisteminin yetkililerce test edilmesi veya korunmasının amaçlandığı hallerde, cezaî yükümlülük doğurmayacağı şeklinde örneklendirilmiştir. Bu durumda "without

[22] Sözleşmeyi hazırlayanlar tarafından çift kullanıma sahip tüm cihazların doğrudan suç sayılması ve doğrudan kapsam dışı bırakılması gibi hususlar tartışılmış; sonuçta, objektif bir şekilde suç işlemek amacıyla oluşturulma ve uyarlanma ölçütü getirilmiştir. Böylelikle çift kullanımlı cihazlar genellikle kapsam dışı tutulmuş olmaktadır. Explanatory Report to the Convention on Cybercrime, p. 73, https://rm.coe.int/16800cce5b E.T: 07.04.2020.

[23] Jonathan CLOUGH, "The Council Of Europe Conventıon On Cybercrıme: Defınıng 'Crıme' In A Dıgıtal World", *Criminal Law Forum* 23, 2012, s.378.

[24] Report, p. 23.

[25] WALDEN, s. 3217.

[26] Report, p. 74.

[27] 18 U.S. Code § 1029(3), https://www.law.cornell.edu/uscode/text/18/1029 E.T: 01.06.2020.

[28] Message From The Presıdent Of The Unıted States, Transmıttıng Councıl Of Europe Conventıon On Cybercrıme (The ''Cybercrıme Conventıon'' Or The ''Conventıon''), Whıch Was Sıgned ByThe Unıted States On November 23, 2001, s.10. https://www.congress.gov/108/cdoc/tdoc11/CDOC-108tdoc11.pdf E.T: 01.06.2020.

right" unsuru yerini "with right" unsuruna bırakır[29]. Özellikle çift kullanımlı araçların cezalandırılmaması adına[30] bu ayrımın açık bir şekilde vurgulanması yerindedir.

Maddenin 3. fıkrası üye devletlerin, Sözleşme'ye bilgisayar şifresi, erişim kodu için çekince konamaz denilmektedir. Bilgisayar şifresi, erişim kodu ve benzeri türden verinin var olabilmesi için onu var edenin herkesin sahip olamayacağı bir bilgi ve beceriye sahip olması gerektiği tartışmasızdır. Bu türden bir var etmenin peşinen kötü niyetli sayılması buna bağlı suçlarla mücadele etmenin önünü açacaktır. Bu bakımdan sözleşmenin böyle bir durumu şart koşması sözleşmenin çıkarılma amacıyla uyumludur.

Sözleşmede öngörülen bu madde temel hazırlık işlemleri niteliğindeki eylemleri cezalandırabilir hale getirmektedir. Sanal suç vasıtalarının çoğalmasıyla oluşan yeraltı pazarları[31] ya da karaborsalar (black market)[32] suçu kaynağında yok etme zorunluluğuna işaret etmektedir. Aksi takdirde, hacker araçları gibi bilgisayar sistemlerini hacklemek için kullanılan elektronik araç pazarlarının büyümesi kaçınılmazdır[33].

B. TCK 245/A DÜZENLEMESİ

"Madde 245/A- (Ek: 24/3/2016-6698/30 md.) (1) 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".

Sözleşmenin kabulünden sonra fakat madde henüz yasalaşmadan önce, uygulamada savcı ve kolluğun bilişim suçlarında hazırlık işlemlerinin cezalandırılmamasının bu suçlarla mücadeleyi imkânsız hale getirdiği yönündeki görüşleri yazıya aktarılmış[34] ve madde malumun ilanı şeklinde düzenlenmiştir. Sözleşme düzenlemesiyle TCK 245/A düzenlemesinin genel olarak uyumlu olduğunu söylemek mümkündür[35]. Maddenin gerekçesinde de sözleşmede geçen unsurlara yer verilmiştir. Alt Komisyonun Değişiklik Gerekçesi şe şekildedir;[36]

"Son olarak 5237 sayılı Kanuna "Yasak cihaz veya programlar" başlıklı 245/A maddesinin eklenmesi öngörülmüştür. Böylece bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bir bilişim suçunun işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal

[29] Report, p. 77.
[30] Jonathan CLOUGH, *PRİNCİPLES OF CYBERCRİME*, Cambridge University Press, 2010, s. 122.
[31] Olgun DEĞİRMENCİ, "Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi", *Yaşar Hukuk Dergisi*, Cilt 1 Sayı 2, 2019, s.190.
[32] Açıklayıcı Rapor, p. 71.
[33] Explanatory Notes to the Police and Justice Act 2006, [303], http://www.legislation.gov.uk/ukpga/2006/48/notes E.T: 28.06.20 20.
[34] Mücahid Özbek, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri*", GSI Articletter Summer 2015, Part 6*, s.81.
[35] Berrin AKBULUT, *Bilişim Alanında Suçlar*, 2. Baskı, Adalet Yayınevi, Ankara, 2017,s. 346. Diğer benzerlik veya farklılıklara konu geldiğince değineceğiz.
[36] TBMM Mevzuat Bilgi Sistemi, https://mevzuat.tbmm.gov.tr/mevzuat/faces/maddedetaylari?psira=122834 E.T: 07.04.2020.

eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran faillerin cezalandırılması amaçlanmaktadır. Mezkûr Sözleşmenin 6'ncı maddesiyle sözleşmeci taraflar, bilişim alanında suç işlenmesini kolaylaştıran cihazların kötüye kullanılmasını cezalandırmaya davet edilmektedir. Bilişim suçları ile bilişim sistemleri araç kılınarak işlenen suçlarla etkin ve caydırıcı bir şekilde mücadele edebilmek için bu tür eylemlerin suç ve ceza politikaları bakımından sınırlandırılması ve yaptırıma bağlanmasında yarar görülmektedir. Maddede tanımlanan suçun oluşumunda kişinin suç işleme kastı dikkate alınmak zorundadır. Buna göre, bu tür cihaz ve programların, bilişim sistemlerinin güvenliğini test etmek amacıyla yapılması veya oluşturulması halinde belirtilen suç oluşmayacaktır. Ayrıca, failin cezalandırılabilmesi bakımından söz konusu cihaz, program, şifre veya güvenlik kodunun suçun işlenmesine elverişli olması gerekir."

Gerekçede; maddenin sözleşmeye uygun olarak çıkartıldığı, bilişim suçları ile bilişim sistemleri araç kılınarak işlenen suçlarla etkin ve caydırıcı olma vasfının amaçlandığı, suçun doğması için kastın şart olduğu, cihaz ve programın suç işlemeye elverişli olması gerektiği gibi hususlar vurgulanmaktadır.

Sözleşme madde 6 ile TCK 245/A arasında iki temel farklılık, doğal olarak, göze çarpmaktadır. İlki, TCK'de suç sayılan eylemler kanunilik ilkesi gereği tek tek yazılırken Sözleşmede eylemler için sınırlayıcı bir tutum sergilenmemiştir[37]. İkinci farklılık, Sözleşme sadece 2 ila 5. Maddeleri işlenmesi yönelik bir suç unsuru belirlemişken, TCK bilişim alanında işlenen suçlara ek olarak bilişim sistemi vasıtasıyla işlenen suçları da 245/A'ya dahil etmiştir[38].

C. DÜZENLENİŞE İLİŞKİN ELEŞTİRİLER

Madde, temel olarak, hızla gelişen teknoloji vasıtasıyla daha riskli hale gelen kötücül yazılım ve cihazların kullanılmasını cezalandırabilmek adına yasal bir zemin sağlamıştır[39]. Dahası, bilişim alanında işlenebilecek suçlara bir set olabilmek adına hazırlık hareketleri olarak adlandırılabilecek eylemleri suç olarak düzenlemiştir[40].

Öğretide, madde başlığının maddenin içeriğini yansıtmak uzak olduğu ve bilişim alanında işlenen suçlar bakımından yetersiz olduğu ileri sürülmektedir[41]. Hatta Özbek, Doğan, Bacaksız "*Suçta kullanılacak cihaz ve programların üretilmesi, yayılması veya bulundurulması*"[42] şeklinde olabileceğini de eklemektedirler. Akbulut, TCK 245'te olduğu gibi "cihaz veya programların kötüye kullanılması" başlığının tercih edilebileceğini[43] ifade etmektedir. Bizce de sözleşme madde 6nın başlığına benzer bir şekilde "cihaz veya programların kötüye kullanılması" tercih edilebilirdi.

Koca/Üzülmez ise maddenin ögelerin değiştirilerek daha kurallı ve sade bir düzenleme olabileceğini göstermektedir. "*Bu bölümde düzenlenen suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesinde kullanmak amacıyla bir cihazı, bilgisayar programını, şifre ve güvenlik*

[37] AKBULUT, s. 346.
[38] AKBULUT, s. 346.
[39] Veli Özer ÖZBEK & Koray DOĞAN & Pınar BACAKSIZ, *Türk Ceza Hukuku Özel Hükümler*, 14. Baskı, Seçkin, Ankara, 2019, s. 1028.
[40] KOCA & ÜZÜLMEZ, s. 913.
[41] KOCA & ÜZÜLMEZ, s. 912, ÖZBEK & DOĞAN & BACAKSIZ, s. 1028-1029.
[42] ÖZBEK & DOĞAN & BACAKSIZ, s. 1029.
[43] AKBULUT, s. 348.

kodlarını üreten, ithal eden, temin eden, satan, satışa arz eden, satın alan veya bulunduran kişi...cezalandırılır."[44]. Bizce de madde ilk bakışta anlaşılmaktan uzaktır. Yapılan eleştirilere rağmen yasak cihaz veya programlar suçu (245/A) esaslı bir eksikliğin tamamladığı kabul edilmelidir[45].

II. YASAK CİHAZ VEYA PROGRAMLAR SUÇU

Yasak cihaz veya programlar suçu, 2016 yılında TCK'de bilişim alanında suçlar başlıklı onuncu bölüme eklenen 245/A maddesi ile yasallaştırılmıştır. Aslına bakılırsa bu suç, maddede belirtilen suçların hazırlık aşamasındaki eylemlerini cezalandıran bir suçtur[46]. Maddeyi ceza hukuku ilkeleri bakımından tahlil etmek gerekmektedir.

Maddede "*münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi*" denilmektedir. TCK kapsamında bilişim suçları, doğrudan bilişim suçları (gerçek bilişim suçları) ve dolaylı bilişim suçları (bilişim bağlantılı suçlar) şeklinde tasnif edilebilir[47]. Buna göre, cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun yapılması veya oluşturulması iki temel kapsamda suç meydana getirir[48].

"Münhasıran bu bölümde yer alan suçlar" ifadesi TCK'de bilişim alanında suçlar başlıklı bölümü belirtir. Buna göre gerçek bilişim suçları; 243 Bilişim sistemine girme, 244: Sistemi engelleme, bozma, verileri yok etme veya değiştirme, 245: Banka veya kredi kartlarının kötüye kullanılması, 246: Tüzel kişiler hakkında güvenlik tedbiri uygulanması şeklindedir.

"Bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar" ifadesi gerek TCK gerekse diğer kanunlarda bilişim sistemlerinin araç olarak kullanıldığı suçları gösterir. Bu başlığı da iki alt başlığa ayırmak mümkündür.

TCK'de bazı suçların "bilişim sistemi" vasıtasıyla işlenmesi nitelikli hal olarak hükme bağlanmıştır[49].142/2/e nitelikli hırsızlık (Bilişim sistemlerinin kullanılması suretiyle), 158/1/f nitelikli dolandırıcılık (Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle) ve 228/3 kumar oynanması için yer ve imkan sağlama (Suçun bilişim sistemlerinin kullanılması suretiyle işlenmesi…) suçları bu şekildedir.

TCK'de ve diğer kanunlarda bazı suçlarda "bilişim sistemi"[50] kavramı kullanılmasa da pratikte suçun gerçekleşmesinde bilişim sistemleri kullanılabilir. Bunlar bakımdan da "bilişim sistemlerinin araç olarak kullanılması suretiyle

[44] KOCA & ÜZÜLMEZ, s. 912.
[45] ÖZBEK & DOĞAN & BACAKSIZ, s. 1028.
[46] KOCA & ÜZÜLMEZ, s. 916.
[47] Metin TURAN, *Bilişim Hukuku*, 4. Baskı, Seçkin, Ankara, 2020, s.68.
[48] Maddenin düzenine göre bu şekilde bir taksim yaptık. Bilişim sistemlerinin kullanılması suçları, nitelikli hal olarak bilişim suçları ve bilişim suçun bir yardımcı unsuru olduğu suçlar şeklinde bir taksim daha anlaşılır olmaktadır. Benzer için bkz. Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt: 71, Sayı: 1, 2013, s. 856.
[49] DÜLGER, 2018, s. 234.
[50] Bu suçların detayları ve bilişim sistemlerinin bu suçların gerçekleşmesindeki işlevi için bkz. AKARSLAN, s.57 vd.

işlenebilen diğer suçlar" kapsamı gerçekleşmiş kabul edilir[51]. Öğretide de haklı olarak savunulduğu üzere[52], maddenin kesin sınırlar belirlemeksizin böyle bir yönlendirmeyle kapsam tayin etmesi kanunilik ilkesine aykırılık noktasında eleştiriye açıktır.

TCK'de bilişim sistemleri vasıtasıyla işlenmeye elverişli bazı suçlara değinmek gerekmektedir. Haberleşmenin engellenmesi, hakaret, haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme, verileri yok etmeme, müstehcenlik, ses veya görüntülerin kayda alınması gibi suçlar sıralanabilir. Aslına bakılırsa, hemen her kaynak farklı suçları da kapsama alabilmektedir. Örneğin, TCK madde 81 ve 82 kasten öldürme ve madde 86 ve 87 kasten yaralama gibi klasik suçlar bile bilişim suçlarıyla işlenmeye elverişli olarak gösterilebilmektedir[53].

Diğer bazı kanunlarda bilişim sistemi ile işlenebilecek bazı suçlara yer vermek istiyoruz. Ancak burada ne tüm kanunların ne de tüm suçların tamamını yazmak mümkün değildir[54].

- Banka Kartları ve Kredi Kartları Kanunu[55];sahte belge düzenlenmesi, gerçeğe aykırı beyan, sözleşme ve eki belgelerde sahtecilik,
- Fikir ve Sanat Eserleri Kanunu[56]; manevi, mali veya bağlantılı haklara tecavüz ve koruyucu programları etkisiz kılmaya yönelik hazırlık hareketler suçları*,
- Elektronik İmza Kanununda[57]; imza oluşturma verilerinin izinsiz kullanımı* ve Elektronik sertifikalarda sahtekârlık suçları,
- Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanununda[58]; İzinsiz faaliyette bulunmak, Denetim ve gözetim faaliyetlerini engellemek ve istenilen bilgileri vermemek, Belgelerin saklanması ve bilgi güvenliği yükümlülüğüne aykırı davranmak suçları,

Bu kapsamda sayılabilecek suçlardır. Burada iki hususu ısrarla vurgulamak gerekir; ilki bu suçlar her işlendiğinde doğrudan 245/A suçu oluşmayacaktır. Bu suçların işlenmesi için cihaz veya yazılım üretilmiş vd. ise 245/A söz konusu olacaktır. Hedef suçun işlenme şeklinden yola çıkarak, her suç ayrı bir tespit gerekecektir. İkinci olarak, bu suçlar sınırlı sayıda gösterilmiş değildir. Bilişim sistemlerinin araç olarak kullanılması gerekli ve yeterli olacaktır.

TCK'de sayılına suçların Sözleşme madde 6da sayılan suçlardan daha geniş olduğunu belirtmekte de fayda vardır. Sözleşmede Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar başlıklı 2 ila 5 maddeleri

[51] GÜL, s. 242.
[52] KORKMAZ, s. 52.
[53] Ebru ALTUNOK & Ali Fatih VURAL, "Bilişim Suçları", *Denetişim*, sayı:8, 2011, s. 80.
[54] Mevzuat için bkz. Dülger, 2019, s. 210-368.
[55] Banka Kartları Ve Kredi Kartları Kanunu, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5464.pdfE.T: 10.04.2020.
[56] Fikir ve Sanat Eserleri Kanunu, https://www.mevzuat.gov.tr/MevzuatMetin/1.3.5846.pdfE.T: 10.04.2020.
[57] Elektronik İmza Kanunu, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf E.T: 10.04.2020.
[58] Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanunun, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6493.pdf .E.T: 10.04.2020.

bu suçun kapsamındadır. Sözleşmede başka suçlara da yer verilmiştir. Örneğin madde 7 ve 8 bilgisayarla bağlantılı sahtecilik ve dolandırıcılık suçları, madde 9 çocuk pornografisi, madde 10 telif haklarına ilişkin suçlar vd. vardır. Cihazların kötüye kullanılması suçu bu suçları da kapsar nitelikle düzenlenmemiştir. Bunun bir ihmal veya gözden kaçırılma olarak değerlendirilmesi güçtür. Diğer bir husus, açıklayıcı raporda yasaların açık ve belirli şekilde düzenlenmesi gerekliliği vurgulanmıştır[59]. Daha önce de bahsettiğimiz üzere, TCK 245/A'nın kapsam bakımından isabetli olmadığını düşünmekteyiz.

İngiltere örneğinde, Bilgisayarların Kötüye Kullanılması Yasası Computer Misuse Act 1990[60] birinci madde, bilgisayara yetkisiz erişim; ikinci madde, başka suçları işlemek veya işlenmesini kolaylaştırmak amacıyla yetkisiz erişim; üçüncü madde, kasten veya bilinçli taksirle bilgisayarın çalışmasına zarar veren fiiller ve 3ZA Ciddi Tehlike Yaratan ya da Buna Neden Olan Yetkisiz fiiller şeklindedir[61]. Madde 3A -2006 yılında eklenmiştir. Yukarda sayılan suçlarda kullanmak veya işlenmesini kolaylaştırmak için araç (article – herhangi bir elektronik biçimde program veya veri) yapma, sağlama (tedarik etme) ve elde etme suçudur. Detayına girmeksizin, madde 3A bizdeki 245/A ile aynı yönde düzenlenmiştir.

Avustralya 'da 2001 tarihli Siber Suç kanunu[62] ile ceza kanununa 476-478 maddeleri (division çevirisi bölüm olsa da kullanım itibariyle maddeye karşılık gelmektedir.) eklenmiştir. Madde 478 (Other computer offences) 3ve4 fıkralar Sözleşmenin 6. Maddesine göre düzenlenmektedir[63]. Madde 478-3; madde 477de düzenlenen suçları (5 yıl ve üzeri tehlikeli suçları işlemek niyetiyle yetkisiz erişim, değiştirme veya bozma) işlemek veya işlenmesini kolaylaştırmak niyetiyle veri bulundurma veya kontrol etme suçudur. "Bulundurma veya kontrol", ilgili verinin ülke içinde veya dışında bulunan ve/veya başkasına ait olan bilgisayarlarda bulunmasını da kapsar. Madde 478-4; bir verinin madde 477de düzenlenen suçları işlemek veya işlenmesini kolaylaştırmak niyetiyle üretme, sağlama ve elde etme suçudur.

Kanada hukukunda[64] bilgisayarın yetkisiz kullanımını ele geçirmek için cihaz bulundurma ve zarar suçu başlıklı 342.2 (1) maddesinde; geçerli bir hukuki neden olmaksızın, madde 342.1 (bilgisayarın yetkisiz kullanımı) veya madde 430 (zarar - bilgisayarla ilgili zarar) suçlarını işlemek niyetiyle oluşturulmuş veya uyarlanmış bir cihazı yapmak, bulunduran, satan, satışa arz eden, ithal eden, kullanmak için elde eden, dağıtan veya erişilebilir kılan kişinin cezalandırılacağı belirtilmiştir.

Alman hukukunda TCK 245/A'ya muvazi düzenleme Bilgisayar Dolandırıcılığı başlıklı 263a maddesidir[65]. Maddenin[66]3. Fıkrasında bilgisayar

---

[59] Açıklayıcı Rapor p. 41. "clarity and specificity" şeklinde ifade edilmektedir.

[60]Computer Misuse Act 1990, http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences E.T: 21.06.2020. biz bu suçların detaylarına elbette girmeyeceğiz. Sadece bizdeki madde ile kıyaslamak adına madde başlıklarına yer verdik.

[61] İngiltere'de bilişim ile ilgili kanun elbette tek değildir. Bundan başka 1964 tarihli "Müstehcen Yayınlar Kanunu", 1984 tarihli "Telekomünikasyon Kanunu" ve 1994 tarihli " Ceza Adaleti ve Kamu Düzeni Kanunu" gibi örnekler mevcuttur. Hüseyin ÇAKIR & Mehmet Serkan KILIÇ,(Ed.) Güncel Tehdit: Siber Suçlar, Seçkin, Ankara, 2014, s. 197.

[62]Cyber Crime Act 2001, https://www.legislation.gov.au/Details/C2004A00937 E.T: 21.06.2020.

[63]The offence provisions of newsections478.3and 478.4 implement Article 6 of the draft Council of Europe Convention on Cybercrime. O dönem henüz sözleşme yürürlüğe girmeği için draft (tasarı) kullanılmıştır. Cybercrime Bill 2001, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd048 E.T: 21.06.2020.

[64]Criminal Code, https://laws-lois.justice.gc.ca/eng/acts/c-46/page-77.html#docCont s.e.t: 22.06.2020.

[65]Metin TURAN, Alman Bilişim Hukuku, Adalet Yayınevi, Ankara, 2011, s. 47.

programları imal etmek, kendisi veya bir başkası için temin etmek, satışa sunmak, bulundurmak veya bir başkasına devretmek suretiyle 1`inci fıkrada belirtilen suçların hazırlık hareketlerini icra eden kişi üç yıla kadar hapis cezası veya adli para cezasıyla cezalandırılır hükmü bulunmaktadır.

Karşılaştırmalı olarak incelediğimiz ülke kanunlarında hedef suçların doğrudan tespit edildiği görülmektedir. Aynı hassasiyete bizim kanun koyucunun da sahip olması beklenirdi. Mevcut durumda suçta ve cezada kanunilik ilkesinin gri kaldığını söylemek mümkündür.

A. KORUNAN HUKUKİ DEĞER

Bilişim sistemine ilişkin suçlarda korunan hukuki değerler, genel olarak, birden fazladır[67]. Korunan hukuki değer, en temel ifadesiyle, bilişim teknoloji sisteminin güvenliğini ve insanların bilişim sistemine olan inancını korumaktır.[68]

TCK 245/A bir taraftan bilişim sistemini ve içerdiği veriyi korurken diğer taraftan bilişim sisteminin vasıta olarak kullanılarak işlenebilecek suçlarda koruna hukuki değerin korunmasında da aracıdır[69].Bu bakımdan dolaylı da olsa, kullanıcıların malvarlığı, özel hayatı ve haberleşme özgürlüğünü vs. korunmaktadır[70].

B. SUÇUN UNSURLARI

TCK'nin suç teorisinde suçun unsurları; maddi unsurlar, manevi unsurlar ve hukuka aykırılık unsurlar şeklinde formüle edilmektedir[71].

1. MADDİ UNSURLARI

Suçun maddi unsurunu; konu, fail, mağdur ve eylem başlıklarında değerlendirmeye tabi tutacağız.

a. Suçun Konusu

Maddede suçun konusu *cihaz, bilgisayar programı, şifre veya sair güvenlik kodu…yapılması veya oluşturulması durumunda* olarak gösterilmektedir.

Maddede geçen kavramları açıklamaya geçmeden evvel bir hususu netleştirmek isteriz. Bilgisayarlar, herkesçe bilineceği üzere, fiziksel ve soyut unsurlardan oluşur. Fiziksel varlığı olan aygıtlar (hardware) donanım ve soyut özelliği kodlar (software)[72] yazılım olarak adlandırılır. Biz de bilgisayar programı, şifre veya sair güvenlik kodu (tek tek veya hepsi) için yazılım kavramını kullanacağız. Cihaz kelimesi kendisinden beklenen imgeyi karşıladığı için ayrıca bir donanım kullanımına başvurmayacağız.

---

[66]Strafgesetzbuch, https://dejure.org/gesetze/StGB/263a.html, E.T: 27.06.2020.
[67] Öğretide var olan tartışmalara girmeksizin kabul ettiğimiz görüş üzerinden açıklama yapmayı uygun buluyoruz.
[68] KOCA & ÜZÜLMEZ, s. 913.
[69] DÜLGER, 2018, s. 454.
[70] GÜL, s. 240.
[71] İzzet GÖNENÇ, *Türk Ceza Hukuku Genel Hükümler*, 15. Bası, Seçkin, Ankara, 2019,s. 178.
[72]Whatarethedifferencesbetweenhardwareand software?https://www.computerhope.com/issues/ch000039.htm. E.T: 10.04.2020.

Bizim ele aldığımız ayırımı kanun koyucu ortaya koymuştur. "Yapmak" fiili cihaza -donanım-, "oluşturmak" fiili bilgisayar programı, şifre veya sair güvenlik koduna –yazılım- uyumlu geldiği için kanun koyucu bu ayrıma özen göstermiştir[73].

Cihaz kavramı; bir bilişim sistemine eklenebilen, bağlanabilen ve istenildiğinde çıkartılmaya elverişli olan fiziksel bir donanımı ifade etmektedir[74]. Bazı cihazlar doğrudan suç işlemeye elverişlidir. Örneğin sözleşmenin 2013 tarihli kılavuzunda, 3. Kişilerin verilerini ele geçirmek amacıyla çok sayıda bilgisayarın birleşerek oluşturdukları ağı (botnet) doğrudan madde 6 kapsamında değerlendirilmektedir[75]. Sözleşme ve TCK cihaz kavramını tanımlamamıştır.

ATM'lere kart kopyalamak için yerleştirilen aparatlar, ATM'lere sokulan kartların şifrelerini okumak için yerleştirilen kameralar[76], kart bilgilerini kopyalayarak sahte kart üretilmesinde kullanılan "encoder"[77], ATM'lere takılan kartların bilgilerini kopyalayan "skimmer"[78]cihaz kavramına örnek[79] teşkil edecektir.

Bilgisayar programı[80] kavramı; kullanıcın haberi ve izni olmaksızın bilişim sistemini ele geçirmeyi[81]ve elde ettiği bilgileri başka bir yere aktarmayı hedefleyen her türlü kötücül yazılımı (malicious software "malware")[82] ifade etmektedir. Virüsler, solucanlar, Truva atı, spam, klavye dinleme sistemleri vs.[83] en bilindik kötücül yazılımlardır. Anlaşılacağı üzere, bilgisayar programları fiziksel bir donanım değil yazılıma ilişkindir[84].

Şifre; sanal âlemde herhangi bir veriye erişimi engellemek veya istenildiğinde erişimi sağlamak için harf, rakam veya diğer semboller ile oluşturulan kilit/anahtardır[85].Bilişim sistemini ele geçirmek veya bilgilere erişmek niyetiyle oluşturulan şifre kırıcı programlar[86] 245/A bakımından suç oluşturacaktır.

Sair güvenlik kodu ise şifre dışında örneğin ses, göz retinası veya parmak okuyucu[87], kredi kartlarının arkasındaki CVV kodu[88]güvenlik önemlerine örnek

---

[73]İrem GEÇMEZ, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m.244), Seçkin, Ankara, 2020, s. 65; BÜK, s. 124.
[74] ÖZBEK & DOĞAN & BACAKSIZ, s. 1029.
[75]Guidance Note on provisions of the Budapest Convention covering botnets, s. 239. https://www.statewatch.org/news/2015/jul/coe-cybercrime-convention-prot-racism.pdf E.T: 10.04.2020.
[76] KOCA & ÜZÜLMEZ, s. 914; ÖZBEK & DOĞAN & BACAKSIZ, s. 1029.
[77] GÜL, s. 240.
[78] AKBULUT, s. 351.
[79] Öğretide bu ve daha fazla cihazı detaylıca anlatan kaynaklar vardır. Biz konuyu dağıtmamak adına sadece en bilinenlerin isimlerini zikrettik.
[80] Bilgisayar programı teriminin kapsamı, virüs programları ya da bilgisayar sistemlerine erişim için tasarlanmış veya uyarlanmış programlar gibi verileri değiştirmek, hatta yok etmek için dizayn edilmiş programlara atıfta bulunur. "*The inclusion of a "computer program" refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virüs programs, or programs designed or adapted to gain Access to computer systems*." (Siber Suçlar Sözleşmesi için Açıklayıcı Rapor) Explanatory Report to the Convention on Cybercrime, 72. Ph. https://rm.coe.int/16800cce5bE.T: 10.04.2020.
[81] ÖZBEK & DOĞAN & BACAKSIZ, s. 1030.
[82] AKBULUT, s. 351.
[83] AKBULUT, s. 352. Biz sadece isim olarak birkaç tanesini yazdık. Okuyucuya referans kitapları önermekteyiz.
[84] Bu yazılımlara örnek vermek konumuz dışındadır. Okuyucu için bkz. DÜLGER, 2018, s. 103 vd.
[85] DÜLGER, 2018, s. 457.
[86] GÜL, s. 240.
[87] DÜLGER, 2018, s. 457.
[88] Diğer türleri için bkz. AKBULUT, s. 353.

teşkil eder. Bu güvenlik önlemleriyle korunan bir programı devre dışı bırakacak kod geliştirilmesi bu kapsamdadır[89].

Sair güvenlik kodu kavramını, tıpkı şifre gibi, sisteme girişte bir araç olarak düşünmek mümkündür ki bu şekilde belirlilik ilkesine ters düşmemesi sağlanmış olur[90].

Bir cihaz veya yazılım birden fazla bilişim suçunu işlemeye elverişli olsa dahi, henüz bir hedef suç işlenmemişse, suç unsuru tek olduğu için tek suç oluşacaktır. Aynı doğrultuda, hedef suçlardan bir veya bir kaçı işlenmişse bu suç(lar) ve 245/A suçu ayrı ayrı oluşacaktır. Hâkim cihazın veya yazılım araçlarının ilgili suçları işleyebilme fonksiyonuna sahip olup olmadığına karar vermeden önce bir uzman görüşüne başvurmalıdır[91].

Son olarak, Sözleşme 6-1-a-ii'de "*bir bilgisayar sisteminin* ***tamamına veya herhangi bir kısmına*** *erişimi mümkün kılan bir bilgisayar şifresi, erişim kodu veya benzer bir veri*" denilmiştir. TCK'de bilişim sistemine girme başlıklı 243. Maddede "Bir bilişim sisteminin bütününe veya bir kısmına" şeklinde bir ifade bulunmaktadır. Ne var ki 245. Madde için böyle bir ayrım yoktur. Yine de bu suçun oluşması için bilişiminin bir kısmına erişimi mümkün kılması yeterli görülmelidir.

b. Fail ve mağdur

Yasak cihaz veya programlar suçu düzenleniş bakımından özel bir niteliğe sahip değildir. Bu bakımdan herkes fail veya mağdur olabilir[92]. Ancak failin sözleşmede/kanunlarda sayılı olan suçları işlemeye elverişli cihaz veya yazılım üretmesi onun herkeste olmayan bir seviyede uzmanlığa sahip olacağı gerçeği göz önünde tutulmalıdır.

c. Eylem

Madde metninde suç konusunu oluşturan bir cihaz, bilgisayar programı, şifre veya sair güvenlik kodunu…*imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran* denilerek eylem unsurları belirlenmiştir[93].

Toplam 11 eylem suçun fiil unsurunu oluşturmaktadır. Bu bakımdan çok hareketli suç denilebilir[94]. Sözleşme madde 6da ise "üretimi, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı veya başka şekilde erişilebilir hale getirilmesi" şeklinde sayılmıştır[95].

- Bu eylemlerden herhangi birini işlemek suçun oluşması için yeterlidir ve bu bakımdan seçimlik hareketli suçtur[96].

[89] BÜK, s. 124.
[90] KOCA & ÜZÜLMEZ, s. 914.
[91] KOCA & ÜZÜLMEZ, s. 914.
[92] KOCA & ÜZÜLMEZ, s. 913; ÖZBEK & DOĞAN & BACAKSIZ, s. 1031.
[93] KOCA & ÜZÜLMEZ, s. 914 (nakletme ile sevk ve depolamak ile bulundurma yakın anlamlarda olduğu için hepsinin kullanılması eleştirilmiştir); ÖZBEK & DOĞAN & BACAKSIZ, s. 1031.
[94] GÖNENÇ, s. 183-184.
[95] Sözleşmenin orijinalinde "or otherwise making available" "veya başka şekilde erişilebilir hale getirme" şeklinde sınırlayıcı olmayan bir tutum gösterilmiştir. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 E.T: 10.04.2020.
[96] KOCA & ÜZÜLMEZ, s. 914; ÖZBEK & DOĞAN & BACAKSIZ, s. 1031.

- Suç sadece sayılı eylemlerle işlenebildiği için yani bunların dışında gerçekleşen eylemler suça sebebiyet vermeyeceği için bağlı hareketli suçtur[97].
- Madde bir zarar şartı koymadığı için suç soyut tehlike suçudur[98].
- Depolamak ve bulundurmak gibi eylemler süreklilik barındırdığı için (eylem devam ettikçe suç işlenmeye devam eder) zamanaşımı veya suçun işleniş anının tespitinde önemlidir[99].

Sayılı eylemlerden iki veya daha fazlasını yapmak yine tek bir suça sebebiyet verirse de temel cezanın belirlenmesinde etkili olacaktır[100].

Maddede sayılan eylem çeşitlerine kısaca değinmek yerinde olacaktır. Ancak şunu hemen belirtmek gerekir ki, 245/A'da sayılan eylemler arasında "yayma" yoktur ve bu öğretide eleştirilmektedir[101].

i. İmal etme

İmal etmek, en basit ifadesiyle üretmek demektir. 245/A bağlamında ise işlevsel açıdan iki yüzü bulunmaktır. Yukarıda bahsedildiği üzere, suçun konu unsurunu cihaz, bilgisayar programı, şifre veya sair güvenlik kodu oluşturur.

Cihaz, fiziksel varlığı olan bir nihai/işlevsel donanımdır. Bu bakımdan, kendisini var eden parçaların –kablo veya elektrik aksamı gibi-teknik işlemlerden geçirilerek cihazın müstakil bir şekilde ortaya çıkması gerekmektedir[102].Diğer taraftan, cihazın parçalarının failin tarafından bizzat üretilmiş olması şart değildir[103].

Bilgisayar programı, şifre veya güvenlik kodu ise yazılıma ilişkindir. Yazılım ilk kez oluşturulabileceği gibi daha önce üretilmiş bir yazılımın kendi başına etkinliği olan bir yaması şeklinde de olabilir[104].

ii. İthal etme

İthal etmek, en yalın ifadesiyle, yurtdışında üretilmiş bir malın yurda yasal yollarla sokulmasıdır. Cihaz son haliyle (mamul) yurda sokulmuşsa ithal kapsamına girecektir; yani parçaları ayrı ayrı bir şekilde getirilip yurtiçinde birleştirilmişse ithal etme eylemi söz konusu olmayacaktır[105].

Yazılım (program, şifre veya sair kodlar) için klasik ithal anlayışını aşmak gerekmektedir. Yazılım bellek gibi bir somut taşıyıcı ile yurda sokulmuşsa ithal edildiği kuşkusuzdur. Fakat yazılım yurtdışında üretilmekle birlikte parası ödenip yurtiçinden kullanılabilir hale gelmişse de ithal edilmiş kabul edilmelidir[106].

[97] ÖZBEK & DOĞAN & BACAKSIZ, s. 1032; bağlı hareketli suçlar bakımından suçun konusun aynı olması gerekmektedir. Detay için bkz. GÖNENÇ, s. 186.
[98] AKBULUT, s. 355.
[99] KOCA & ÜZÜLMEZ, s. 914.
[100] KOCA & ÜZÜLMEZ, s. 914.
[101] AKBULUT, s. 357.
[102] ÖZBEK & DOĞAN & BACAKSIZ, s. 1032.
[103] AKBULUT, s. 355.
[104] ÖZBEK & DOĞAN & BACAKSIZ, s. 1032.
[105] ÖZBEK & DOĞAN & BACAKSIZ, s. 1032.
[106] ÖZBEK & DOĞAN & BACAKSIZ, s. 1032.

iii. Nakletme ve sevk etme

Nakletmek, sözlük itibariyle, "*bir yerden başka bir yere geçirmek, iletmek, anlatmak, aktarmak*" gibi anlamlara gelmekte iken sevk etmek ise "*göndermek, götürmek"* manalarını barındırmaktadır[107].

Maddenin yorumu olarak ise nakletme mevzu bahis cihaz, bilgisayar programı, şifre veya sair güvenlik kodunu alıcıya bizzat teslim etmeyi; sevk etme ise bunları bir aracı vasıtasıyla göndermeyi ifade etmektedir[108]. Yazılım unsurlarının ağ sistemiyle iletilmesi de nakletme veya sevk etme olarak değerlendirilir[109].

Maddede ithal durumunun zaten düzenlenmiş olmasına binaen nakletme ve sevk etme eylemlerinin hem yurtiçinde gerçekleşmeyi hem de ihracatı kapsadığı düşünülebilir[110].

iv. Depolama ve bulundurma

Sözlükte hem fiziki bir biriktirmeyi hem de bir verinin bellek cihazına konulmasını ve saklanmasını karşılamaktadır[111]. Madde de aynı anlamı barındırmaktadır. Cihazın fiziksel olarak bir yerde, bilgisayar programı, şifre veya sair güvenlik kodunun ise sanal/dijital ortamda erişime her an açık olacak bir şekilde tutulmasıdır[112]. Depolama; bilgisayar programı, şifre veya sair güvenlik kodu bakımından alelade bir kayıttan nitelik, amaç, boyut gibi yönlerden farklı olup bunlara ilişkin her otomatik kayıt 245/A kapsamında değerlendirilemez[113].

Bulundurma, depolama ile yakın/ortak kümesi olan ve fakat ondan daha geniş boyutlara sahip bir kavramdır. Bulundurma; kişinin cihaz, bilgisayar programı, şifre veya sair güvenlik kodu ile mekânsal ve zamansal bir yakınlıkta bulunmasa bile onlara istediği takdirde ulaşma imkânı sağlayan hâkimiyet sahası[114] şeklinde anlaşılabilir.

Sözleşmede taraf devletlere, bulundurma eyleminin gerçekleşmesi bu tür öğelerden belli bir sayıda olması şartını koyma imkânı tanınmıştır. Kanun koyucu bulundurma ile ilgili böyle bir yol izlememiştir.

v. Satma, satın alma ve satışa arz etme

Satma ve satın alma, aralarında ticari saik ile iş yapan tarafların eylemlerini ifade eder. Cihaz veya yazılımın bir değer karşılığında, kullanılması için gerekli şifre veya kodlarla birlikte el değiştirmesidir[115].

Madde bağlamında satışa arz etme, ilgili cihaz, bilgisayar programı, şifre veya sair güvenlik kodunu karşı tarafın olası alış iradesine cevap verebilecek bir aşama/durum/iradeyi işaret etmektedir[116].

[107]Türk Dil Kurumu Sözlükleri, https://sozluk.gov.tr/ E.T: 10.04.2020.
[108] ÖZBEK & DOĞAN & BACAKSIZ, s. 1033.
[109] AKBULUT, s. 356.
[110] ÖZBEK & DOĞAN & BACAKSIZ, s. 1033.
[111]Türk Dil Kurumu Sözlükleri, https://sozluk.gov.tr/ E.T: 10.04.2020.
[112] ÖZBEK & DOĞAN & BACAKSIZ, s. 1033.
[113] ÖZBEK & DOĞAN & BACAKSIZ, s. 1033.
[114] ÖZBEK & DOĞAN & BACAKSIZ, s. 1034.
[115] AKBULUT, s. 356.

vi. Kabul etme ve başkalarına verme

Kabul etme ve başkalarına verme; satma ve satın almanın aksine, aralarında ticari anlamda bir bedel/karşılık olmaksızın ilgili cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun el değiştirilmesine[117] denir.

Sözleşmede üretim, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı veya başka şekilde erişilebilir hale getirilmesi şeklinde bir eylem sıralaması yapılmaktadır.

d. Suça etki eden nedenler

Maddede yasak cihaz ve programlar suçunu hafifleten ve ağırlaştıran nedenler gösterilmemiştir.

2. SUÇUN MANEVİ UNSURU

Yasak cihaz veya programlar suçu, kast ile işlenmeye elverişli olup taksir ile işlenmesi mümkün değildir[118]. Madde bağlamında kastın tespiti çok önemlidir. Failin cihaz veya yazılım araçlarına ilişkin sayılı eylemleri, mezkûr suçları işlemek amacıyla icra etmiş olması şarttır[119].

Manevi unsur tespit edilirken, oluşturulan cihaz veya yazılımın yapılış biçimi ve niteliği gibi unsurlara bakılır; gerekmesi halinde bir uzmandan görüş alınabilir[120].Ayrıca failin bu cihaz ve yazılımın maddede belirtilen suçların işlenmesiyle ilgili olduğunu da bilmesi gerekir[121].

Madde sayılı eylemlerin bir veya birkaçını (nakletme gibi) yapan failin maddede belirtilen cihaz veya yazılımlara ilişkin teknik bilgisinin olmadığı tespit edilirse, bu suçu işlemiş sayılamaz[122].AKBULUT doğrudan kastın sadece yapma veya oluşturma ile ilgili olduğunu diğer fiillerin işlendiği durumda fail için olası kastın söz konusu olabileceğini ifade etmektedir[123].

3. HUKUKA AYKIRILIK UNSURU

Maddede kapsamında suç olmaya elverişli durum; kamu otoritesinin izni ve yasal bir yetkinin kullanılması[124]halinde suç gerçekleşmez. Örneğin, CMK madde 134 "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" kapsamında yapılacak işlemler görevin ifası olduğu için hukuka uygun sayılacaktır[125].

Sözleşme madde 6-2 bir tür hukuka uygunluk örneği vermektedir. "*2 ila 5. maddeler uyarınca suç işlemek maksadıyla gerçekleştirilmemesi durumunda,*

[116] ÖZBEK & DOĞAN & BACAKSIZ, s. 1033.
[117] ÖZBEK & DOĞAN & BACAKSIZ, s. 1033.
[118] ÖZBEK & DOĞAN & BACAKSIZ, s. 1034.
[119] KOCA & ÜZÜLMEZ, s. 915.
[120] GÜL, s. 241.
[121] AKBULUT, s. 358.
[122] GÜL, s. 242.
[123] AKBULUT, s. 358.
[124] KOCA & ÜZÜLMEZ, s. 915.
[125] AKBULUT, s. 359.

örneğin bir bilgisayar sisteminin yetkililerce test edilmesi veya korunmasının amaçlandığı hallerde, cezaî yükümlülük doğuracağı şeklinde yorumlanmayacaktır."

TCK 245/A maddesinin gerekçesinde de hukuka uygunluk durumuna değinilmiştir. "*Bu tür cihaz ve programların, bilişim sistemlerinin güvenliğini test etmek amacıyla yapılması veya oluşturulması halinde belirtilen suç oluşmayacaktır*." denilmektedir.

Her iki durumu da bir örnekle[126] açıklamak gerekirse, bir kişinin bilgisayarında yazılı suçları işlemeye elverişli şifre kırıcı veya casus programlar gibi bulunursa cezalandırılabilirken bu kişi bilişim sistemi güvenliğinde çalışan biriyse cezalandırılmaz[127].

Unutulmamalıdır ki, salt bu cihaz veya yazılımları yapmak suçu doğurmaz. Bunların belirtilen suçlarda kullanılması ayırıcı niteliktir.

Maddenin düzenlenişi itibariyle, meşru müdafaa ve ilgilinin rızası hukuka uygunluk sebeplerinin, bu madde bağlamında geçerli olmadığı yönünde görüş bulunmakla birlikte biz ilgilinin rızasının belli bir olay özelinde gerçekleşebileceğini dolayısıyla dolasıyla mümkün olduğunu düşünmekteyiz[128].

C. YAPTIRIM VE YARGILAMA USULÜ

Maddede "*bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır*." denilmektedir. Kanun koyucu bir yandan hapis cezası diğer taraftan adli para cezası öngörmüştür. TCK'deki bu tercih, genellikle, işlenen suçun neticesinde bir ekonomik getiri varsa söz konusu olmaktadır[129].

Adli para cezasında üst sınır belirlenmiş olmakla birlikte alt sınır belirlenmemiştir. Bu durumda TCK madde 52 devreye girecektir ve 5 günden az olmayacaktır[130].

İngiltere'de, suçlamaya bağlı olarak, 2 yıla kadar hapis veya para cezası ayrı ayrı veya birlikte uygulanacak şekilde düzenlenmektedir. Avustralya'da 3 yıl hapis cezası (Cezalandırılan hedef suçların cezası en az 5 yıldır.) öngörülmektedir. Almanya'da 3 yıla kadar hapis veya adli para cezası ve Kanada'da 2 yıla kadar hapis cezasına karar verilebilmektedir.

Yaptırıma ilişkin bir takım tutarsızlıklar bulunmaktadır. 245/A azami 3 yıl ve 5 gün para cezası öngörürken maddenin kapsamına giren suçlardan özellikle TCK

---

[126] Benzer bir örnek, açıklayıcı raporda da vardır. Örneğin, test cihazları ("şifre-kıran cihazlar") ve bilgi teknolojileri ürünlerinin güvenirliliğini kontrol etme ya da sistem güvenliğini test etme amacıyla sektör tarafından üretilen ağ analiz cihazları, yasal amaçlar doğrultusunda üretilir ve bunu aklı selimin tercihi olacağı düşünülür. "*For example, test-devices ("cracking-devices") and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'*". Explanatory Report to the Convention on Cybercrime, 77. Ph.

[127] GÜL, 241-242.

[128] AKBULUT, s. 358-359. Ancak ilgilinin rızası bakımından, bilişim güvenliği üreten bir firma başka bir firmayla sisteminin güvenliğini test etmesi için anlaşmış olabilir. Böyle özel örneklerde ilgilinin rızasının varlığını kabul etmek gerekir. Pantest (sızma testi) için bkz. BGA Security,10 Soruda Sızma Testi Nedir?,https://www.bgasecurity.com/2017/09/10-soruda-sizma-testi/ E.T: 10.04.2020.zaten hem sözleşme hem gerekçede bu tip durumların cezalandırılamayacağı açıkça yazılıdır.

[129] KOCA & ÜZÜLMEZ, s. 916.

[130] AKBULUT, s. 362.

madde 243 Bilişim sistemine girme suçunda öngörülen cezalar " 1 yıla kadar", " 1. Fıkranın yarısı kadar", "2 yıla kadar" ve "3 yıla kadar" şeklindedir. Bu durumda, hazırlık aşamasındaki ceza asıl cezadan fazla hale gelebilmektedir[131]. 245/A için asgari sınır belirlemeksizin hedef suçun cezasına endeksli bir düzenleme yapılmış ve hakimin bu olmasının daha uygun olacağını söylemek mümkündür.

Suçun soruşturması ve kovuşturması resen yapılacaktır; ayrıca bir şikâyete tabi değildir[132]. Yargılama, cezanın üst sınırı 3 yıl olduğu için, Asliye Ceza Mahkemesinin görev alanındadır[133].

Suç, temel olarak, sırf hareket suçu olduğu için eylemin yapıldığı yer mahkemesi yetkili iken kesintisiz suç, zincirleme suç veya teşebbüs durumları varsa yetkili mahkeme CMK'ye göre tespit edilecektir[134].

D. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

Teşebbüs; failin maddede yazılı seçimlik hareketlerden birine başladıktan sonra kendi iradesi dışında bir sebeple hareketi tamamlayamama ihtimali (örneğin üretim devam ederken polis baskının gerçekleşmesi ve üretimin durması[135]) bulunduğundan suça teşebbüs mümkündür[136] demek yerinde olacaktır. Teşebbüs kabul edildiği takdirde gönüllü vazgeçmenin de kabulü mümkündür[137].

Suça iştirak; maddede sayılan bazı eylemler tek bazıları çok faille[138] işlenebilecektir[139]; fakat maddede iştirake ilişkin özel bir hüküm olmadığı için genel hükümler geçerlidir[140]. Örneğin, sisteme girmeksizin ağlar arasında veri akışını izlemek amacıyla teknik olanak sağlayan kişi, eğer bu suçun faili ile ortak suç işleme kararıyla hareket etmiş ise, her ikisi de TCK 243/4'teki suçun birlikte faili olarak cezalandırılırken teknik olanak sağlayan kişi iştirak iradesiyle hareket etmiş değilse, onun açısından uygulanacak hüküm m. 254A olacaktır.[141] Satmak-satın almak veya devretmek-kabul etmek çok failli suç niteliğinde olduğundan hareketlerden biri yapıldığında her iki fail de cezalandırılacaktır. Başka bir örnekte, satma fiilinde satın alan kişi de m. 245/2'den sorumlu tutulacaktır. Sahte kartın üretilmesinde kullanılan bir cihazın temin edilmesinde ise TCK m. 245/A gerçekleşecektir. Aynı zamanda cihazı temin eden kişi m. 245/2'ye yardım eden

---

[131] Durmuş TEZCAN & Mustafa Ruhan ERDEM & Murat ÖNOK, Teorik ve Pratik Ceza Özel Hukuku, Güncellenmiş 17. Baskı, Seçkin, Ankara, 2019, s. 1064.
[132] KOCA & ÜZÜLMEZ, s. 916.
[133] DÜLGER, 2018, s. 460.
[134] CMK; "*Yetkili mahkeme Madde 12 – (1) Davaya bakmak yetkisi, suçun işlendiği yer mahkemesine aittir. (2) Teşebbüste son icra hareketinin yapıldığı, kesintisiz suçlarda kesintinin gerçekleştiği ve zincirleme suçlarda son suçun işlendiği yer mahkemesi yetkilidir*." "*Özel yetki Madde 13 – (1) Suçun işlendiği yer belli değilse, şüpheli veya sanığın yakalandığı yer, yakalanmamışsa yerleşim yeri mahkemesi yetkilidir*." "*Yetkide olumlu veya olumsuz uyuşmazlık Madde 17 – (1) Birkaç hâkim veya mahkeme arasında olumlu veya olumsuz yetki uyuşmazlığı çıkarsa, ortak yüksek görevli mahkeme, yetkili hâkim veya mahkemeyi belirler."* AKBULUT, s. 362-363. Biz hususta daha fazla bilgi vermeden referans kitapları önermekteyiz.
[135] KOCA & ÜZÜLMEZ, s. 915.
[136] AKBULUT, s. 360; ÖZBEK & DOĞAN & BACAKSIZ, s. 1035.
[137] AKBULUT, s. 360; ÖZBEK & DOĞAN & BACAKSIZ, s. 1035.
[138] Kabul etme ve başkalarına verme; satma ve satın alma çok failli karşılaşma suçlarıdır. Bkz. GÖNENÇ, s. 529.
[139] AKBULUT, s. 360.
[140] KOCA & ÜZÜLMEZ, s. 915; ÖZBEK & DOĞAN & BACAKSIZ, s. 1035.
[141] TEZCAN & ERDEM & ÖNOK, s. 1064.

konumunda olacaktır. Cihazı veren kişi m. 245/A'nın faili olduğundan failliğin şerikliğe üstünlüğü ilkesi gereğince m. 245/A'dan sorumlu olacaktır[142].

Suçların içtimaı; suçu oluşturan seçimlik hareketlerden bir veya birkaçını yapmak tek suç oluşturur[143]. Fail, seçimlik hareketlerden biri vasıtasıyla sahip olduğu cihaz veya yazılım ile hedef suçlardan birini işlerse hem bu suçlardan hem de 245/A'dan ayrı ayrı cezalandırılır[144]. İçtima ile ilgili ilginç bir durum TCK 243/4te yaşanmaktadır. "*Öte yandan bu suçla TCK madde 245A arasındaki ilişki asıl norm – yardımcı norm ilişkisi olup TCK 243/4ün uygulandığı durumlarda faile ayrıca m.245A'dan ceza verilemez. Bu durum, verileri izleyen kişinin teknik olanağı hazırlayan kişiden daha az cezalandırılmasını sağlamaktadır ki, bu yönüyle mevcut düzenleme eleştirilmelidir"*.[145] Suçu işleyenin suça hazırlık eyleminde olandan daha az cezalandırılması gibi bir durum yaşanabilmektedir.

Belli bir sayıda üretip elinden çıkardıktan sonra yeniden üretirse zincirleme suç oluşabilecektir[146].

E. ÖZEL HÜKÜMLER

Yasak cihaz veya programlar suçu TCK'de düzenlenmiş olmakla genel hüküm niteliğindedir. Odaklandığı eylemler maddede belirtilen suçların hazırlık işlemleri niteliğindeki eylemlerdir. Ancak TCK'ye göre özel kanun sayılacak diğer bazı kanunlarda da hazırlık işlemlerinin cezalandırılacağına ilişkin hükümler mevcuttur. Bu hükümlerin çatışması halinde genel norm-özel norm ilkesi gereği TCK 245/A devre dışı kalacaktır[147].

İlk örnek, Fikir ve Sanat Eserleri Kanunu; "*Koruyucu programları etkisiz kılmaya yönelik **hazırlık hareketleri**, madde 72- (Değişik: 23/1/2008-5728/139 md.) 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*."

İkinci örnek, Elektronik İmza Kanunu, "*İmza oluşturma verilerinin izinsiz kullanımı Madde 16- (Değişik: 23/1/2008 – 5728/525 md.) **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*."

Üçüncü örnek, Elektronik Haberleşme Kanunu[148], "*madde 63 (4) 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*

[142] Berrin AKBULUT, "Banka Veya Kredi Kartlarının Kötüye Kullanılması", *Yaşar Hukuk Dergisi*, Cilt 1 Sayı 2 2019, s. 34.
[143] ÖZBEK & DOĞAN & BACAKSIZ, s. 1035.
[144] KOCA & ÜZÜLMEZ, s. 916; ÖZBEK & DOĞAN & BACAKSIZ, s. 1035.
[145] TEZCAN & ERDEM & ÖNOK, s. 1064.
[146] KOCA & ÜZÜLMEZ, s. 916.
[147] AKBULUT, s. 361.
[148] Elektronik Haberleşme Kanunu, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdfE.T: 10.04.2020.

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."

Dördüncü örnek, Karayolları Trafik Kanunu[149], "*madde 51/4* ***Hız sınırlarının aşılıp aşılmadığını, tespit etmekte kullanılan cihazların yerini tespit veya sürücüyü ikaz eden her türlü cihazın imalı, ithali ve araçlarda bulundurulması yasaktır***."

Dört örnekte de bilişim sistemleriyle ilgili bir takım eylemler suç kapsamına alınıp cezalandırılmaktadır. Biz burada detaylandırmadık ama hükümler, 245/A maddesine göre özel hükümdür ve olası çatışma halinde cari olmaya devam edecektir. Son olarak, ceza mevzuatımızda bu örneklerden başkaları da olabileceğini eklemek isteriz.

SONUÇ

Teknolojinin ve internetin hızla gelişmesi beraberinde birçok sıkıntıyı da getirmiştir. Kişilerin ve kurumların güvenlikleri siber (bilişim) yollarla ihlal edilmeye başlanmıştır. Bu durum devletleri harekete geçmeye itmiştir.

Uluslararası düzeyde Avrupa Konseyi Siber Suç Sözleşmesi bilişim yoluyla işlenebilecek suçların önüne geçmek adına imzalanmıştır. Mevcut durumda birçok ülke bu sözleşmeyi imzalamış ve kendi iç hukuklarında uygun düzenlemeleri yürürlüğe sokmuştur.

Türkiye 2010 yılında imzaladığı sözleşmeyi 2014 yılında kanunlaştırarak yürürlüğe sokmuştur. Sözleşmeye uyum sağlama doğrultusunda çok sayıda değişiklik yapılmış. 2016 yılında yapılan değişiklikle TCK'ye yasak cihaz veya program suçu başlıklı 245/A maddesi bilişim alanında işlenen suçlar bölümüne eklenmiştir.

TCK 245/A maddesi sözleşmenin 6. Maddesine dayanılarak ihdas edilmiştir. Maddenin başlığı ve içyapısı ilişkin eleştiriler mevcuttur. Kanun koyucunun bu hususta bir adım atması beklenebilir.

TCK 245/A maddesi ile ilk olarak, bilişim teknoloji sisteminin güvenliğini ve insanların bilişim sistemine olan inancını koruma amaçlanmaktadır. Madde, işlenmesini engellediği suçta korunan hukuki değeri de dolaylı olarak korumaktadır.

Maddede suçun konusu "cihaz, bilgisayar programı, şifre veya sair güvenlik kodu… yapılması veya oluşturulması durumunda" gerçekleşir. Fail ve mağdur herkes olabilir. Fail; imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran şeklinde ortaya çıkar.

Suçun kapsamında doğrudan bilişim suçları ve dolaylı bilişim suçları yer almaktadır. Doğrudan bilişim suçları TCK'de 243-246 arasında düzenlenmiş suçlardır. Dolaylı bilişim suçları maddede "bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen" şeklinde tarif edilmektedir. Bizce bu durumda dolaylı bilişim suçlarının ne olduğu belirsizdir. Bizce kanun koyucu dolaylı bilişim suçlarını ya tek tek yazarak göstermeli ya da temel bir formül ile bu suçların tespitini mümkün kılmalıdır. Aksi takdirde, kanunilik ilkesi gölgelenmiş olacaktır.

[149] Karayolları Trafik Kanunu, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2918.pdfE.T: 10.04.2020.

Suçun manevi unsuru kasttır. Bilinçli taksirle işlenmesi mümkün değil iken olası kastla işlenmesi hususu tartışmalıdır. Suç maddede gösterilen suçları işlemek amacıyla harekete geçilmesi durumunda meydana gelir. Yasal bir emri yerine getirme ve ilgilinin rızası (tartışmalı) gibi hukuka uygunluk nedenleri kabul edilmiştir.

Suçun işlenmesi halinde 1 yıldan 3 yıla kadar hapis cezası ve 5.000 güne kadar adli para cezası öngörülmüştür. Suç resen soruşturulur, Asliye Ceza Mahkemelerinde görülür. Suça ilişkin teşebbüs, iştirak gibi hususlarda farklı bir özellik görülmezken hedef suçun işlenmesi halinde her iki suçtan ayrı ayrı (gerçek içtima) ceza verilir.

TCK 245/A maddesi bazı suçların hazırlık işlemleri niteliğindeki eylemleri cezalandırmaktadır. Bu işlevi ile oldukça istisnai bir örnektir. Düzenlendiği yer ceza kanunu olduğu için bazı özel kanunlarda yer alan maddelerle çatışması halinde uygulanması kalkar.

Yüksek yargı organları önüne gelmiş yeteri kadar hüküm, maalesef, yoktur. Yargının maddeye bakışını şimdiden tahmin güçtür fakat bizce maddeden çıkması olası sorunlar çoktur. Eylemlerin hazırlık işlemleri niteliğinde olması şüpheden ari bir kanaate ulaşmanın önüne geçmeye dolasıyla cezalandırmaya engel durumlar yaratmaya açıktır.

KAYNAKÇA

AKARSLAN Hüseyin, *Bilişim Suçları*, 2. Baskı, Seçkin, Ankara, 2015.

AKBULUT Berrin, "Banka Veya Kredi Kartlarının Kötüye Kullanılması", *Yaşar Hukuk Dergisi*, Cilt 1 Sayı 2 2019.

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

ALİUSTA Cahit & BENZER Recep, "Avrupa Siber Suçlar Sözleşmesi Ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt:4, No:2, S:35-42, 2018.

ALTUNOK Ebru & VURAL Ali Fatih, "Bilişim Suçları", *Denetişim*, Sayı8, 2011.

BÜK Alaattin, *Bilişim Alanında Kişisel Verilerin Korunması*, Seçkin, Ankara, 2018.

CLOUGH Jonathan, "A World Of Dıfference: TheBudapestConventıon On CybercrımeAndTheChallenges Of Harmonısatıon", *MonashUniversityLawReview* (Vol 40, No 3),2014.

CLOUGH Jonathan, "TheCouncil Of Europe Convention On Cybercrime: Defining 'Crıme' In A Dıgıtal World", *CriminalLaw Forum* 23, 2012.

CLOUGH Jonathan, *Principles Of Cybercrime*, Cambridge UniversityPress, 2010.

ÇAKIR Hüseyin & KILIÇ Mehmet Serkan,(Edi) Güncel Tehdit: Siber Suçlar, Seçkin, Ankara, 2014.

DEĞİRMENCİ Olgun, "Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi", *Yaşar Hukuk Dergisi*, Cilt 1 Sayı 2, 2019.

DEMİRCAN Tunç, *Bilişim Alanında Suçlar,* Legal Yayıncılık, İstanbul, 2016.

DÜLGER Murat Volkan, *Bilişim, Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı*, 5. Baskı,Seçkin, Ankara, 2019.

DÜLGER Murat Volkan *Bilişim Suçları ve İnternet İletişim Hukuku*, 7. Baskı, Seçkin, Ankara, 2018.

ERDAĞ Ali İhsan, "Bilişim Alanında Suçlar (Türk Ve Alman Ceza Hukukunda)", *Gazi Üniversitesi Hukuk Fakültesi Dergisi* Cilt: XIV, Sayı 2, 2010.

ERDOĞAN Yavuz, *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargı Kararları İle)*, Legal Yayıncılık, İstanbul, 2013.

GEÇMEZ İrem, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m.244), Seçkin, Ankara, 2020.

GİLES Keir, *Prospects For The Rule Of Law In Cyberspace*, Strategic Studies Instituteand U.S. Army War College Press, 2017.

GÖNEN Serkan & ULUS Halil İbrahim & YILMAZ Ercan Nurcan, "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme", *Bilişim Teknolojileri Dergisi*, Cilt 9, Sayı 3, 2016.

GÖNENÇ İzzet, *Türk Ceza Hukuku Genel Hükümler*, 15. Bası, Seçkin, Ankara, 2019.

GÜL Ahmet, *Doğrudan/Dolaylı Bilişim Suçları*, 2. Baskı, Seçkin, Ankara, 2018.

İÇEL Kayıhan, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri"", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt 59, Sayı 1-2, 2001.

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

KORKMAZ İbrahim, "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu", *Terazi Hukuk Dergisi*, Cilt 13 sayı 142, 2018.

KURNAZ Salim & ÖNEN S. Mustafa, "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri", *International Journal of Politicsand Security*, Cilt 1, Sayı 2, 2019.

MAHMUTOĞLU Fatih S., "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt 59, Sayı 1-2, 2001.

MAHMUTOĞLU Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt 71, Sayı 1, 2013.

ÖNOK Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,(Prof.Dr. Nur Centel'e Armağan)*,Cilt 19, Sayı 2, 2013.

ÖZBEK Mücahid, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri*", GSI Articletter,,Part 6* 2015.

ÖZBEK Veli Özer & DOĞAN Koray &BACAKSIZ Pınar, *Türk Ceza Hukuku Özel Hükümler*, 14. Baskı, Seçkin, Ankara, 2019.

SOKULLU-AKINCI Füsun, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt 59, Sayı 1-2, 2001.

TEZCAN Durmuş & ERDEM Mustafa Ruhan & ÖNOK Murat, Teorik ve Pratik Ceza Özel Hukuku, Güncellenmiş 17. Baskı, Seçkin, Ankara, 2019.

TURAN Metin, Alman Bilişim Hukuku, Adalet Yayınevi, Ankara, 2011.

TURAN Metin, *Bilişim Hukuku*, 4. Baskı, Seçkin, Ankara, 2020.

VATİS Michael A.,"The Council of Europe Convention on Cybercrime", *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, NationalAcademiesPress, 2010.

VİANO Emilio C. "Cybercrime: Definition, Typology, and Criminalization",*Cybercrime, Organized Crimeand Societal Responses, International Approaches (Ed. Emilio C. Viano),*Springer Nature, Cham, Switzerland 2017.

WALDEN Ian, "Harmonising ComputerCrimeLaws in Europe*", European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 12, Issue 4, 2004.

İnternet Erişimli Kaynaklar

18 U.S. Code § 1029(3), https://www.law.cornell.edu/uscode/text/18/1029 E.T: 07.04.2020.

BGA Security,10 Soruda Sızma Testi Nedir?,https://www.bgasecurity.com/2017/09/10-soruda-sizma-testi/

Computer Misuse Act 1990, http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offencesE.T: 21.06.2020.

Convention on Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561E.T: 04.04.2020.

Criminal Code, https://laws-lois.justice.gc.ca/eng/acts/c-46/page-77.html#docCont E.T: 22.06.2020.

Cybercrime Act 2001, https://www.legislation.gov.au/Details/C2004A00937E.T: 21.06.2020.

Cybercrime Bill 2001, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd048 E.T: 21.06.2020.

Explanatory Report totheConvention on Cybercrime, https://rm.coe.int/16800cce5bE.T: 07.04.2020.

ExplanatoryNotestothePoliceandJusticeAct 2006, [303], http://www.legislation.gov.uk/ukpga/2006/48/notes E.T: 28.06.20 20.

GuidanceNote on provisions of theBudapestConventioncoveringbotnets, s. 239. https://www.statewatch.org/news/2015/jul/coe-cybercrime-convention-prot-racism.pdf E.T: 07.04.2020.

Strafgesetzbuch, https://dejure.org/gesetze/StGB/263a.html, E.T: 27.06.2020.
TRANSMITTING ...https://www.congress.gov/108/cdoc/tdoc11/CDOC-108tdoc11.pdf E.T: 07.04.2020.

Türk Dil Kurumu Sözlükleri,https://sozluk.gov.tr/E.T: 10.04.2020.

Whatarethedifferencesbetweenhardwareand software? https://www.computerhope.com/issues/ch000039.htm. E.T: 07.04.2020.