Makale Türü/Article Type: Araştırma

BİLİŞİM ALANINDA SUÇLARIN VEYA BİLİŞİM SİSTEMLERİNİN ARAÇ OLARAK KULLANILDIĞI DİĞER SUÇLARIN İŞLENMESİ AMACIYLA CİHAZ, PROGRAM, ŞİFRE YA DA GÜVENLİK KODLARININ ÜRETİLMESİ, YAYILMASI VEYA BULUNDURULMASI SUÇU

The Crime of Production, Proliferation or Possession of Devices, Computer Programs, Passwords or Security Codes in Order to Commit Cybercrimes or other Criminal Offences in Which Information Systems are Used as Tools

Dr. Öğretim Üyesi Ahu KARAKURT EREN*

Geliş Tarihi: 10.03.2020 Kabul Tarihi: 04.06.2020

ÖZET

Türk Ceza Kanunu'nun (TCK) 245/A maddesinde "Yasak Cihaz veya Programlar" başlıklı hüküm ile teknolojik gelişmelerle giderek yaygınlık kazanan bilişim suçlarıyla ve bilişim sistemlerinin araç olarak kullanıldığı diğer suçlarla henüz bu suçlar işlenmeden mücadele etmek hedeflenmektedir. Çünkü TCK'nın 245/A maddesinde, bilişim suçlarının ve bilişim sistemlerinin kullanılması suretiyle işlenen diğer suçların hazırlık hareketi vasfı taşıyabilecek fiiller bağımsız suç olarak tipikleştirilmiştir. Aslında kanun koyucunun bu tercihi, pek çok suçun işlenmesine ortam ve malzeme hazırlayan hacker araçlarının kara borsalarının uluslararası pazarlar haline gelmesi nedeniyle varılmış olan uluslararası uzlaşıyla bağlantılıdır. Çünkü TCK'nın 245/A maddesi, Türkiye'nin de taraf olduğu Siber Suç Sözleşmesi'nin 6. maddesinde öngörülen suç haline getirme yükümlülüğünü karşılamaya yöneliktir. Bu makalede öğretide ileri sürülen görüşler dikkate alınarak bilişim alanında suçların veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre

ABSTRACT

The provision titled 'Illegal Devices & Computer Programs' under Article 245/A of Turkish Criminal Code targets to combat with cybercrimes which gradually spread along with technological developments and also other criminal offences in which information systems are used as tools even before such type of crimes are committed. That is because of the fact that, in Article 245/A of Turkish Criminal Code, actions which are likely to be preparatory in nature for committing cybercrimes and other criminal offences in which information systems are used are characterized as substantive crimes. The predilection of the law-maker in this direction pertains to the international consensus reached along with the internationalization of black markets for hacking tools which create the platform and equipment necessary for the perpetration of several criminal offences. That is due to the fact that Article 245/A of Turkish Criminal Code is intended for fulfilling the obligation to prescribe a crime which is in compliance with the criminal offence stipulated in the Sixth Article of the Convention on Cybercrime to which Turkey is also Party. By taking into consideration the views which are expressed

* İzmir Demokrasi Üniversitesi Hukuk Fakültesi, e-posta: ahu.karakurt@idu.edu.tr, ORCID ID: 0000-0001-6384-2166.

veya güvenlik kodlarının üretilmesi, yayılması ya da bulundurulması suçu incelenecektir. Mevcut düzenleme biçimi ile TCK'nın 245/A maddesinin ceza hukukunun temel ilkeleriyle uyumu tartışılacaktır. Olması gereken hukuk açısından somut öneriler geliştirilmeye çalışılacaktır.

Anahtar Kelimeler: bilişim sistemlerinin güvenliği, bilişim alanında suçlar, bilişim sistemleri aracıyla işlenen suçlar, hacker araçları, kanunilik ilkesi, yasak cihaz ve programlar.

in legal doctrine, this paper will analyze the crime of production, proliferation or possession of devices, computer programs, passwords or security codes for perpetrating cybercrimes or other criminal offences in which information systems are used as tools. If Article 245/A of Turkish Criminal Code in its current regulation form conforms to the basic principles of criminal law will be discussed. Attempts will be made to develop concrete proposals in the sense of lex ferenda.

Key Words: security of information systems, cybercrimes, crimes committed via information systems, hacking tools, legality principle, illegal devices & computer programs

GİRİŞ

Bilişim alanındaki gelişmeler bireysel ve toplumsal yaşamı kolaylaştırıcı ve geliştirici etkiler yaratabilmektedir. Bu sebeple bilişim sistemleri her geçen gün hayatın tüm alanlarına artan oranda dahil edilmektedir. İfade edilen durum, toplumsal yaşamın devamlılığını bilişim sistemlerinin işlerliğinin sağlanmasına ve bilişim sistemlerinin güvenliği ile güvenilirliğine olan inancın teminine bağlı kılmaktadır. Bilişim alanındaki gelişmelerin bir diğer sonucu ise bilişim sistemleriyle ilgili güvenlik risklerinin artması ve yeni suç yöntemlerinin keşfidir. Belirtilen sonuç bilişim sistemlerinin işlerliğini sekteye uğratabileceği gibi bilişim sistemlerinin güvenliği ile güvenilirliğine olan toplumsal inancı da zedeleyebilir. Bu durum toplumsal yaşamın sürdürülebilirliği bakımından tehlike yaratacağından, bilişim sistemlerinin güvenliği ve güvenilirliğine yönelik risklerin en aza indirilmesi önemli bir toplumsal ihtiyaç haline gelmiştir.

Belirtilen ihtiyaca yönelik olarak son çare olma özelliği bulunan ceza hukuku araçlarından yararlanmak da dahil olmak üzere devletlerin aldığı tedbirler yetersiz kalmaktadır. Çünkü bilişim alanındaki gelişmeler ülkesel sınır ve mesafe kavramlarını adeta etkisizleşmektedir. Bu durum, siber suçlarla uluslararası mücadeleye girişilmesini zorunlu kılmıştır. Avrupa Konseyi nezdinde imzaya açılan Türkiye'nin de tarafı olduğu Siber Suç Sözleşmesi[1], ifade edilen uluslararası mücadelenin somut bir örneğidir. Siber Suç Sözleşmesinde devletler arası düzenleme farklılıkları nedeniyle bazı fiillerin cezasız kalması tehlikesini bertaraf etmeye yönelik olarak taraf devletlerin maddi ceza hukuklarını birbirlerine yaklaştırmasını sağlamak üzere yer verilmiş hükümler bulunmaktadır[2]. Bu düzenlemelerden birisi Sözleşmenin "Cihazların Kötüye Kullanımı" başlıklı 6. maddesinde yer almaktadır. Söz konusu hükümde, uluslararası çapa ulaşan hacker araçlarının kara borsasının ortadan kaldırılması amacına yönelik olarak Sözleşmenin diğer maddelerinde düzenlenerek taraf

---

1 Türkiye'nin taraf olduğu bu Sözleşmenin adı, Sözleşmenin uygun bulunmasına ilişkin 6533 sayılı Kanunda ve ekinde Sanal Ortamda İşlenen Suçlar Sözleşmesi olarak ifade edilmiştir. Ancak Sözleşmenin İngilizce metinde Sözleşmenin adı "Convention on Cybercrime" olduğundan çalışmada öğretide de kullanıldığı üzere Sözleşme, Siber Suç Sözleşmesi olarak adlandırılacaktır. Bu kullanıma örnek olarak bkz. Kayıhan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, C.59, S.1-2, 2001, s.3 vd; Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Özel Sayı Prof. Dr. Nur Centel'e Armağan*, C.19, S.2, 2013, s.1229 vd; Cahit Aliusta ve Recep Benzer, "Avrupa Siber Suç Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, C.4, S.2, 2018, s.35 vd.

2 Siber Suç Sözleşmesinin hedeflerinden birinin taraf devletlerin maddi ceza hukuklarını birbirine yaklaştırmak olduğuna ilişkin tespit için bkz. Council of Europe, *Explanatory Report to the Convention on Cybercrime ETS 185*, https://rm.coe.int/16800cce5b, (11.12.2019), s.4.

devletlerin suç haline getirmesi gerektiği belirtilen yasa dışı erişim, yasadışı müdahale, verilere müdahale ve sisteme müdahale fiillerinin hazırlık hareketi vasfı taşıyan hareketlerin taraf devletlerce suç haline getirilmesi yükümlülüğü öngörülmektedir.

Sözleşmenin 6. maddesinde öngörülen yükümlülüğü karşılamaya yönelik olarak hukukumuzda bulunan düzenleme TCK'nın Bilişim Alanında Suçlar Bölümüne 2016 yılında eklenen TCK'nın 245/A maddesidir. Ancak söz konusu hükmün olan ve olması gereken hukuk bakımından pek çok yönüyle tartışılması gerekmektedir. Çünkü Siber Suç Sözleşmesi'nin 6. maddesinde taraf devletler için suç haline getirilme yükümlülüğü öngörülen fiiller ile TCK'nın 245/A maddesinde tipikleştirilen fiiller kıyaslandığında TCK'nın 245/A maddesinin çok daha geniş kapsamlı olduğu görülmektedir. Bu durum, kanun koyucunun suç tipini geniş düzenlemek şeklinde ortaya koyduğu tercihinin sonuçlarının ne olduğunu ve düzenlemenin ceza hukukunun temel ilkelerine uyumlu olup olmadığını tartışmaya değer bir hale getirmektedir.

TCK'nın 245/A maddesi ilişkin yapılması gerekliliğine inandığımız tartışmaya bir nebze olsun katkı sağlamak amacıyla makalenin konusu "Bilişim Alanında Suçların veya Bilişim Sistemlerinin Araç Olarak Kullanıldığı Diğer Suçların İşlenmesi Amacıyla Cihaz, Program, Şifre veya Güvenlik Kodlarının Üretilmesi, Yayılması ya da Bulundurulması Suçu" olarak belirlenmiştir. Aşağıda öğretide ileri sürülen görüşlere yer verilerek öncelikle suçla korunan hukuki değer ele alınacaktır. Daha sonra TCK'nın 245/A maddesi hükmü ile Siber Suç Sözleşmesi'nin 6. maddesi kıyaslamalara da işaret edilerek suç unsurlarına ayrılarak incelenecektir. Suç tipi açısından teşebbüs, iştirak, içtima konuları ve yaptırım meselesi ele alınacaktır. Ulaşılan sonuçlar olması gereken hukuk açısından değerlendirilmeye çalışılacaktır.

I. GENEL AÇIKLAMA

Yasak cihaz ve programlar başlıklı TCK'nın 245/A maddesi hükmü hukukumuzda kişisel verilerin korunması açısından mevcut eksikliği gidermek için yasalaştırılan 24.03.2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesiyle oluşturulmuştur.

Öğretide hükmün başlığı eleştirilmektedir· Katıldığımız bu eleştirilerin özünde; cihaz ve programların suçun konusunu teşkil ettiği, kanunun sistematiği göz önünde bulundurulduğunda madde başlıklarının seçiminde suçun eylem unsurunun ön plana çıkarıldığı, 245/A maddesinin bu esasla tezat teşkil ettiği, madde içerisinde cihaz veya programın yasaklı olmasına işaret eden bir ifadenin bulunmadığı ve dolayısıyla başlığın madde içeriğini

yansıtmaktan uzak olduğu tespitleri yer almaktadır[3]. Getirilen eleştirilere ilişkin olarak olması gereken hukuk açısından madde başlığının "suçta kullanılacak cihaz ve programların üretilmesi, yayılması ve bulundurulması" şeklinde tercih edilmesinin daha isabetli olacağı belirtilmektedir[4].

TCK'nın 245/A maddesinin başlığı suç tipinin adını yansıtmaktan da uzaktır. Bu nedenle olsa gerek öğretide suç tipinin isimlendirilmesinde iki farklı tercihler söz konusudur. Bu tercihler, cihaz, program, şifre ve güvenlik kodlarının bilişim suçlarının işlenmesi amacıyla imal ve ticareti suçu[5] ve yasak cihaz veya programların üretilmesi ve ticareti suçu[6] olarak sıralanabilir.

Aşağıda inceleneceği üzere suçla yasaklanan eylemden hareketle suç tipini bilişim alanında suçların veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre ya da güvenlik kodlarının üretilmesi, yayılması veya bulundurulması suçu şeklinde isimlendirmeyi uygun bulmaktayız.

II. SUÇLA KORUNAN HUKUKİ DEĞER

Öğretide TCK'nın 245/A maddesiyle tipikleştirilen suçla korunan hukuki değerin ne olduğu tartışmalıdır. İleri sürülen bir görüşe göre suçla korunan hukuki değer kamunun bilişim sistemlerine yönelik güvenidir[7]. Diğer görüşler suç ile birden fazla hukuki değerin korunduğu konusunda uzlaşsa da bu değerlerin ne olduğu konusunda farklılar içermektedir. Bu kapsamda ileri sürülen bir görüş suçla korunan hukuki değerleri; toplum güvenliği, özel hayat, malvarlığı ve haberleşme özgürlüğü olarak sıralamaktadır[8]. Diğer bir görüşe göre suçla korunan hukuki değerler, bilişim sistemlerinin güvenilirliği ve güvenliği ile kamu düzen ve güvenliğidir[9]. Başka bir görüş yukarıda sıralanan hukuki değerlere ek olarak bilişim suçları ve bilişim yoluyla işlenen suçların koruduğu hukuki değerler arasında bulunan özel yaşamın gizliliği,

---

3 Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, 14. Baskı, Ankara 2019, s.1028 vd; Aynı yönde bkz. Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 7. Baskı, Ankara 2018, s.454; Berrin Akbulut, *Bilişim Alanında Suçlar*, 2. Baskı, Ankara 2017, s.348.

4 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1029; Öğretide Akbulut ise TCK'nın 245/A maddesinde 245. maddede tercih edilen başlığa benzer şekilde program veya cihazların kötüye kullanılması başlığının kullanılmasının daha uygun olacağı görüşündedir. Bkz. Akbulut, s.348.

5 İbrahim Korkmaz, "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu", *Terazi Hukuk Dergisi*, C.13, S.142, Haziran 2018, s.45

6 Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, 6. Baskı, Ankara 2019, s.912; Dülger, s.452.

7 Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 913.

8 Ahmet Gül, *Doğrudan - Dolaylı Bilişim Suçları*, 2. Baskı, Ankara 2018, s.240.

9 Akbulut, s.349.

dokunulmazlığı ve haberleşme özgürlüğünün de suçla korunduğunu ifade etmektedir[10]. Bir diğer görüş korunan hukuki değerleri; bilişim sistemlerinin güvenilirliği ve güvenliği, kişilerin kendilerini özgürce geliştirebilme hakkı ve bilişim teknolojileri kullanıcılarının uğrayacakları zararlar bakımından malvarlığı değerleri olarak sıralamaktadır[11]. Aktarmak istediğimiz son görüşe göre ise suçla korunan hukuki değerler, bilişim sistemlerine karşı toplumda oluşan güven ve 245/A maddesindeki araçlarla işlenecek diğer suçların koruduğu hukuksal değerlerdir[12].

Yukarıda belirtiğimiz tartışma açısından görüşümüzü açıklamak gerekirse bilişim suçları ve bilişim sistemlerinden faydalanmak suretiyle işlenen diğer suçlarda da kullanılabilen hacker araçlarına ilişkin kara borsanın varlığı yadsınamayacak bir gerçektir. Avrupa Konseyi nezdinde hazırlanıp imzaya açılan Siber Suç Sözleşmesinin 6. maddesiyle bu gerçeğin uluslararası düzeyde açıkça kabul edildiği söylenebilir[13]. Söz konusu kara borsanın varlığının, toplumsal ve bireysel hayatta kişilerin ve kurumların bilişim sistemlerinin yaygın kullanımı, satın alınan veya satılan hacker araçlarıyla işlenebilecek suçlar dikkate alındığında haberleşme özgürlüğü, özel yaşamın dokunulmazlığı, kişilerin kendilerini özgürce geliştirebilme hakkı, malvarlığı değerleri ve kamu düzeni açısından risk oluşturabileceği ortadadır. Ancak bu tespite dayanarak TCK'nın 245/A maddesiyle doğrudan korunan hukuki değerlerin sıralanan değerler olduğunu söylemek mümkün değildir. Çünkü TCK'nın 245/A maddesiyle tarif edilerek suç haline getirilen davranışlar, bilişim alanında işlenen suçların ve bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen diğer suçların hazırlık hareketleridir[14]. Salt bu davranışlar, doğrudan haberleşme özgürlüğüne, özel yaşamın dokunulmazlığına, kişilerin kendilerini özgürce geliştirebilme hakkına ve malvarlığı değerlerine yönelik tehlike ya da zarar oluşturmaya elverişli değildir. Söz konusu davranışlar genel olarak kişisel verilerin hukuka aykırı olarak ele elde edilmesini teminine yönelik imkan oluşturmakta ve bu suretle bilişim sistemlerinin güvenilirliği ve güvenliği açısından tehlikeye neden olmaktadır. Ortaya konulan tespiti TCK'nın 245/A maddesinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesiyle oluşturulmuş olması ve hükmün TCK'da düzenlenme yeri (TCK'nın Topluma Karşı Suçlar kısmının Bilişim Alanında Suçlar Bölümü) desteklemektedir. Bu nedenle TCK'nın 245/A maddesiyle düzenlene suçla korunan hukuki değerin birden çok

---

10 Korkmaz, s.49.

11 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1029.

12 Dülger, s. 456.

13 Bkz. Council of Europe, *Explanatory Report to the Convention on Cybercrime ETS 185*, s.12.

14 Bu suçun işlenmesi amaçlanan suçlar bakımından hazırlık hareketi niteliğinde olan fiillerin cezalandırmasına yönelik bir suç olduğu tespit için bkz. Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 916; Dülger, s. 459; Akbulut, s.348; Korkmaz, s.53.

olduğu yönündeki öğretide yapılan yukarıda aktardığımız tespite katılmaktayız ve suçla kişisel verilerin güvenliği ile bilişim sistemlerinin güvenilirliği ve güvenliğinin korunduğu görüşündeyiz.

III. SUÇUN UNSURLARI

A. Tipe Uygunluk Unsuru

1. Objektif Nitelikteki Unsurlar

a. Fail ve Mağdur

Bilişim alanında suçların veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre ya da güvenlik kodlarının üretilmesi, yayılması veya bulundurulması suçu, düzensiz çok failli suç[15] vasfı taşımaktadır. Çünkü TCK'nın 245/A maddesinde yer alan seçimlik hareketlerden bir bölümü (imal etmek, bulundurmak, satışa arz etmek, nakletmek, depolamak, sevk etmek) bir tek fail tarafından gerçekleştirilebilir nitelikte iken, bir bölümü (satmak- satın almak, başkasına vermek- kabul etmek, ithal etmek) zorunlu olarak birden fazla failin suça katılımıyla gerçekleştirilmesi mümkün olan eylemlerdendir[16]. Bu tespit iştirak açısından işlevsel olup, iştirak konusu incelenirken tekrar ele alınacaktır.

Öte yandan suçun failinin bir özellik taşıması, örneğin bilgisayar ya da bilişim alanında uzman olmasına gerek bulunmamaktadır· Herkesin suçun faili olması mümkün olduğundan[17] suç, özgü suç vasfı taşımamaktadır.

Suçun faili bakımından son olarak Türk hukukunda tüzel kişilerin cezai sorumlulukları bulunmadığı için bir tüzel kişinin bu suçun fail olamayacağına dikkat çekmek gerekir.

Bilişim alanında suçların veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre ya da güvenlik kodlarının üretilmesi, yayılması veya bulundurulması suçuyla korunan hukuki değer yukarıda belirtiğimiz üzere kişisel verilerin güvenliği ile bilişim sistemlerinin güvenilirliği ve güvenliğidir. Bu hukuki değerler belli bir kişiye olmayıp, toplumunun geneline aittir. Dolayısıyla suçun mağduru toplumu oluşturan herkestir[18].Şifre veya güvenlik kodunun somut bir kişiye ait olması

---

15 Düzensiz çok failli suç kavramı için bkz· Türkan Yalçın Sancar, *Çok Failli Suçlar*, Ankara 1998,113 vd; Timur Demirbaş, *Ceza Hukuku Genel Hükümler*, 14. Baskı, Ankara 2019, s.498.

16 Suçun bazı seçimlik fiiller bakımından suçun çok failli suç özelliği taşıdığı yönünde bkz· Akbulut, s·350; Dülger, s·456; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.913; Korkmaz, s.49.

17 Gül, s·240; Akbulut, s·349; Dülger, s·456; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.913; Korkmaz, s.49; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1031.

18 Öğretide suçla korunan hukuki değer konusunda farklılıklar mevcutsa da hakim görüş suçun mağdurunun toplumu oluşturan herkes olduğu ve mağdurun belli bir kişi olmadığı

halinde bu kişinin de suçtan zarar gören olduğunu kabul etmek gerekir. Suçun mağdurunun kim olduğu sorusuna verilen yanıt, özellikle 245/A maddesinde tipikleştirilen suç bakımından hukuka uygunluk nedenlerinden rıza açısından değerlendirmede bulunurken işlevsel olacaktır. Tekrara düşmemek için ilgili başlıklar altında yapılan açıklamalara atıf yapmak ile yetinmekteyiz.

b. Suçun Maddi Konusu

Suçun maddi konusu; münhasıran bilişim alanında işlenen suçların veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesinde kullanılmak üzere yapılmış ya da oluşturulmuş olmak kaydıyla cihaz, bilgisayar programı, şifre veya sair güvenlik kodudur[19].

Tek bir güvenlik kodunun ya da şifrenin veya cihazın suçun konusunu teşkil etmesi mümkündür. Oysa Siber Suç Sözleşmesinin 6. maddesinde taraf devletlerin suç haline getirme yükümlülüğü yerine getirirken bulundurma eylemi yönünden cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun belli sayıda bulundurulmasını suçun oluşması bakımından bir şart olarak öngörebilecekleri ifade edilmiştir. Ancak Türk kanun koyucu suçun maddi konusu bakımından böyle bir sınırlamaya gitmeyi uygun bulmamıştır. Kanımızca 245/A maddesiyle hacker araçlarının kara borsasının önlenmesinin amaçlandığı düşünüldüğünde kanun koyucunun tercihinin yerinde olduğu söylenebilir. Ancak bulundurma ve depolama eylemleri açısından failin amacı yönünden sıklıkla belirleme güçlüğü yaşanacağı aşikardır ki bu durum şüpheden sanık yararlanır ilkesinin ihmal edildiği bir uygulamada kusur prensibi ile çelişen kararlara neden olabilir[20]. Ayrıca ceza hukukunun ikincillik ilkesi ile bağdaşmayan sonuçlara sebebiyet verebilir. İfade edilen nedenle

yönündedir. Bkz. Gül, s.240; Dülger, s.456; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.913; Akbulut, s.350; Korkmaz, s.49; Öte yandan öğretide Özbek, Doğan ve Bacaksız, suçun faili ve mağduru açısından özellik göstermediği, suçun failinin ve mağdurunun herkes olabileceği tespitlerinde bulunmaktadırlar. Suçun hukuka aykırılık unsuru açısından yaptıkları açıklamalarda ise bu suç bakımından ilgilinin rızasının hukuka uygunluk nedeni teşkil edebileceği sonucuna ulaşmaktadırlar. Aktarılan tespitler bir arada değerlendirildiğinde Özbek, Doğan ve Bacaksız'ın görüşlerinin suçun mağdurunun belli bir kişi olduğu şeklinde yorumlanmasının mümkün olduğu söylenebilir. Bkz. Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1031, 1034.

19 Dülger, s. 456 vd; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.913 vd; Akbulut, 354; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1029 vd; Gül, s. 240; Korkmaz, s.49.

20 TCK'nın 245/A maddesinde suç teşkil eden hareketlerin çok geniş kapsamlı olarak düzenlenmiş olması ve özellikle yazılımların bulundurulması fiilinin da suç kapsamına alınması nedeniyle hükmün uygulanmasında sızma testleri ile ilgili olarak pek çok tartışma ve sorunun yaşanacağı tespit ve öngörüsü için bkz. Merve Erdem ve Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C.68, S.1, 2019, s.188 vd

suçun maddi konusu açısından bulundurma ve depolama eylemleriyle sınırlı olmak üzere suçun maddi konusuna ilişkin bir sayı şartı getirilmesi önerisi yerinde bir çözüm olarak değerlendirilebilir[21].

Suçun maddi konusu açısından aşağıda önce cihaz, bilgisayar programı, şifre, sair güvenlik kodu terimlerinin anlamı ele alınacak, sonra münhasıran bilişim alanında işlenen suçlar veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesinde kullanılmak üzere yapılmış ya da oluşturulmuş olmak koşulu tartışılacaktır.

(1) Cihaz

Türk Dil Kurumu'nun Güncel Türkçe Sözlüğüne göre cihaz, "*alet, aygıt, takım*" anlamına gelmektedir[22]. Türkçe Bilim Terimler Sözlüğünde ise terim, kelime anlamıyla aynı olmak üzere "*aygıt*"[23] şeklinde tanımlanmıştır.

TCK'nın 245/A maddesi açısından ise cihaz kavramı bilişim sistemlerinin donanım unsuru esas alınarak anlamlandırılmaktadır. Bu bağlamda cihaz, bilişim sistemine eklenebilen, bağlanabilen ve ihtiyaç durumunda çıkarılabilen, ancak bilişim sistemine mutlak suretle bağlı kalacak nitelikte olması zorunluluğu bulunmayan donanım unsuru şeklinde tanımlanabilir[24].

Cihaz kavramına öğretide banka ve kredi kartlarının kopyalanmasında kullanılan manyetik kart kopyalama aparatları(skimmer), sahte klavye (PINPAD), elde edilen bilgileri boş plastik kartların sarkasındaki manyetik seriye yüklemeye yarayan kodlayıcı (encoder), ATM'ye yerleştirilen şifrelerin çalınması için kullanılan kamera düzenekleri örnek gösterilmektedir[25].

Öğretide bir cihazın incelediğimiz suçun konusu olabilmesi bakımından mutlaka ileri teknoloji gerektiren cihazlardan olmasına gerek bulunmadığı

---

21 Amerika Birleşik Devletlerinde federal suçlara ilişkin Amerika Birleşik Devletleri Düsturu'nun 18. Başlığı altında yer alan 1029. maddede en az on beş ya da daha fazla sahte ve yetkisiz erişim araçlarının bulundurulmasının suç haline getirildiğine ilişkin bkz. Dülger, s.458, dn.628.

22 Türk Dil Kurumu, *Güncel Türk Sözlük*, https://sozluk.gov.tr/, (11.12.2019).

23 TÜBA, *Türkçe Bilim Terimleri Sözlüğü*, http://www.tubaterim.gov.tr/, (11.12.2019).

24 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1030; Aynı yönde bkz. Akbulut, s. 350; Korkmaz, s.49 vd.

25 Bu örnekler için bkz. Akbulut, s. 350 vd; ATM'lere takılan kart kopyalama aparatı (skimmer) ve ATM'ye yerleştirilen şifrelerin çalınması için kullanılan kamera düzenekleri örneği için bkz. Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1030; ATM'lere takılarak kullanılan kart kopyalama aparatı ile POS cihazı benzeri kart kopyalama aparatı örneği için bkz. Dülger, s.457; ATM'lere takılarak kullanılan kart kopyalama aparatı örneği için bkz. Korkmaz, s.50; Kart kopyalama aparatları, kodlayıcı, sahte klavye, ATM'ye yerleştirilen şifrelerin çalınması için kullanılan kamera düzeneği hakkında kısa, fotoğraflı açıklama için bkz. Türkiye Bankalar Birliği, *Bankacılıkta Dolandırıcılık Eylemleri, Tespit ve Önleme Yöntemleri*, https://www.tbb.org.tr/gec/KTPV14.pdf, (11.12.2019), s.62 vd.

ifade edilmektedir[26]. Bununla birlikte kanımızca bir bilişim sisteminin olağan şekilde çalışmasına etki eden her aracın da cihaz olarak kabulü mümkün değildir. Örneğin ATM'lerde para veya kart sıkıştırmakta kullanılan saç tokası benzeri basit düzenekler[27], sahte kart basmakta kullanılabilen salt beyaz plastik kartlar kanımızca cihaz olarak değerlendirilemez. Aksinin kabulü halinde cihaz kavramı yaklaşık olarak her şey ile eş anlamlı hale gelir. Bu TCK'nın 254/A maddesinde "bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar" ifadesine yer verildiği de gözetildiğinde cezalandırılabilir davranışların sınırını kabul edilemez ölçüde genişleten bir yorum olur.

Cihaz kavramı açısından ele alınması gereken bir diğer soru cihazın yasak olmasının suçun konusunu teşkil edebilmesi bakımından gerekip gerekmediğidir. Her ne kadar madde başlığında yasak ifadesine yer verilmiş olsa da TCK'nın 245/A maddesinde cihazın yasak olması gerektiği yönünde bir açıklamaya yer verilmemiştir. Madde başlıkları bağlayıcı olmadığından ve hükümde de cihazın yasaklılığına ilişkin bir düzenlemeye yer verilmediğinden cihazlar yönünden yasak olma koşulu ile suçun konusunu sınırlamak mümkün değildir[28]. Aksi yöndeki bir değerlendirme hükmün amacıyla bağdaşmayacak şekilde dar yorumlanmasına yol açacaktır. Örneğin yukarıda belirtilen kamera açısından hükmü uygulamak olanaksız hale gelecektir.

(2) Bilgisayar Programı

Türkçe Bilim Terimler Sözlüğünde bilgisayar programı "*Belirli bir işi gerçekleştirmek üzere gerekli işlemlerin belirli bir programlama dilinde yazılmış komutlar dizisi hali*"[29] şeklinde tanımlanmaktadır.

Siber Suç Sözleşmesinin 6. maddesinde de bu kavrama yer verilmiş olup, Sözleşmenin bağlayıcı olmayan Açıklama Raporunda söz konusu kavram, "*istenen sonucu elde etmek için bilgisayar tarafından yürütülebilen bir dizi komut"*[30] olarak tanımlanmıştır.

Öğretide TCK'nın 245/A maddesinde kullanılan bilgisayar programı kavramı ise aynı maddede yer verilen bilişim alanında işlenen suçlar veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesinde kullanılmak üzere yapılmış ya da oluşturulmuş olmak koşulu nedeniyle olsa

---

26 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1030.

27 Örnek resimler için bkz. Türkiye Bankalar Birliği, *Bankacılıkta Dolandırıcılık Eylemleri, Tespit ve Önleme Yöntemleri,* s.60.

28 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1028 vd.

29 TÜBA, *Türkçe Bilim Terimleri Sözlüğü*, http://www.tubaterim.gov.tr/, (11.12.2019).

30 Bkz. Council of Europe, *Explanatory Report to the Convention on Cybercrime ETS 185*, s.5.

gerek, zararlı (kötücül) yazılımlar olarak anlamlandırılmaktadır[31]. Bilişim sahibi tarafından izin verilmeyen işlemleri gerçekleştiren yazılımlar olarak tanımlayabileceğimiz zararlı yazılımlara; bilgisayar virüsleri (dosya virüsleri, boot sector virüsleri, multipartite virüsler, makro virüsler, betik virüsler gibi), solucanlar (ağ ve elektronik posta solucanları), Truva atları, casus yazılımlar (arka kapılar, keylogger, rootkit), fidye yazılımlar, sahte güvenlik yazılımları[32] örnek gösterilebilir.

(3) Şifre

Türkçe Bilim Terimler Sözlüğünde şifre "*açık bir metnin karakterlerinin bir algoritma uygulanarak başka karakterlerle yer değiştirilmesi ya da bu karakterlerin sıralarının değiştirilmesi gibi yöntemlere dayanarak metnin içeriğini gizlenmesi ya da bu işleme tabi tutulmuş metin*" şeklinde tanımlanmıştır[33].

Siber Suç Sözleşmesinin 6. maddesinde bir bilgisayar sisteminin tamamına ya da bir kısmına erişimi mümkün kılan bilgisayar şifresi kavramına yer verilmiştir. Ne Sözleşmede ne de Sözleşmenin bağlayıcı olmayan Açıklama Raporunda kavramın içeriğine ilişkin bir açıklamaya yer verilmemiştir. Ancak bununla birlikte "bir bilgisayar sisteminin tamamına ya da bir kısmına erişimi mümkün kılan" nitelendirmesi terimin anlamlandırılmasında yol göstericidir.

TCK'nın 245/A maddesinde kullanılan şifre kavramı için erişim ile ilgili bir nitelendirme yapılarak özelleştirilmiş olmasa da öğretide kavramın içeriğinin tespitinde şifrenin erişime ilişkin fonksiyonundan hareket edildiği ve dar yorumlandığı söylenebilir. Çünkü öğretide şifrenin sayı ya da sembolden oluşturulan dijital kilitler olup, gizli kalması istenen belge, bilgi veya sistemlere ulaşılmasını sağlayan anahtar şeklinde anlamlandırıldığı[34] görülmektedir.

Öğretide şifreleme işleminin bir yazılımla desteklendiği, dolayısıyla şifreleme işleminin bir programlama olarak kabul edilebileceği ifade edilmekte, şifre kavramının belirsiz olduğu, kanun koyucunun ne tür şifreleri suçun konusu olarak kabul ettiğini izah etmesinin yerinde olabileceği eleştirisi yapılmaktadır[35]. Katıldığımız bu eleştiri bakımından Siber Suç Sözleşmesinin 6. maddesinde tercih edilen "bir bilgisayar sisteminin tamamına ya da bir kısmına

---

31 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1030; Akbulut, s.551 vd; Korkmaz, s.50.

32 Zararlı yazılım türleri için bkz. Ömer Çıtak, *Ethical Offenssive- Defensive Hacking*, 11. Baskı, İstanbul 2019, s.112 vd.

33 TÜBA, *Türkçe Bilim Terimleri Sözlüğü*, http://www.tubaterim.gov.tr/, (11.12.2019).

34 Dülger, s.457.

35 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1031.

erişimi mümkün kılan" ifadesinden yola çıkarak bir öneri geliştirilebilir[36]. Kanaatimizce şifre ifadesinin önünde "bir bilişim sisteminin tamamına ya da bir kısmına erişimi mümkün kılan" nitelendirmesi eklenerek TCK'nın 245/A maddesi hükmünün yeniden formüle edilmesi kanunilik ilkesinin belirlilik esasına uygun bir çözüm olabilir.

(4) Sair Güvenlik Kodu

Türk Dil Kurumu'nun Güncel Türkçe Sözlüğünde güvenlik kodu tanımlanmamış olsa da güvenlik ve kod kelimelerin ayrı ayrı tanımları bulunmaktadır. Bu bağlamda güvenlik kelimesi için yer verilen tanım "*toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet*" iken kod kelimesi için verilen tanımlar "*harf*" ve "***şifre***" şeklindedir[37].

Türkçe Bilim Terimler Sözlüğünde ise güvenlik kodu teknik bir terim olarak tanımlanmış değildir. Ancak kod "*bir veri kümesinin tüm öge veya simgelerine bir standarda göre bağlanan sayısal karşılıkların bütünü*" şeklinde tanımlanmaktadır[38].

Siber Suç Sözleşmesinin 6. maddesinde "erişim kodu ve benzeri veri" ifadesine yer verilmiştir. Sözleşmede ve Sözleşmenin bağlayıcı olmayan Açıklama Raporunda bu kavrama açıklık getirilmemiştir. Ancak Sözleşmede kod kelimesinin önünde kullanılan erişim ifadesi terimin anlamlandırılmasında sınırlayıcı bir işlev görebilir niteliktedir.

TCK'nın 245/A maddesinde ise sair güvenlik kodu ifadesi tercih edilmiştir. Öğretide sair güvenlik kodunun bilişim teknolojisi güvenliğini sağlamak için oluşturulmuş ilave kodları anlattığı ifade edilmektedir[39]. Şifre dışında güvenlik amacıyla kullanılan ses, retina, parmak ya da avuç izi tanıma gibi özellik barındıran güvenlik unsurları[40], kredi kartlarının arka yüzünde yer alan CVC2 ya da CID denilen güvenlik kodları örnek gösterilmektedir[41].

Öğretide ileri sürülen bir görüşe göre şifre ifadesi gibi sair güvenlik kodları ifadesinin de neyi anlattığı belirsizdir. Bu eleştiri kanun koyucunun ne tür

---

[36] Bu bağlamda karşılaştırmalı hukukta Alman Ceza Kanunu'nun 202c maddesinden yararlanmak mümkündür. Çünkü Alman Ceza Kanunu'nun 202a ve 202b maddelerinde düzenlenen veri casusluğunun ve verileri ele geçirme suçlarının hazırlık hareketlerinin tipikleştirildiği 202c maddesi, TCK'nın 245/A maddesinin kısmen karşılığı olarak değerlendirilebilir. Bu hükümde Alman kanun koyucu suçun konusunu saptarken şifre ve sair güvenlik kodu ifadesini "verilere giriş yapmayı sağlayan" nitelendirmesiyle sınırlamayı uygun görmüştür. Bu tercih Siber Suç Sözleşmesinin 6. maddesindeki düzenlemeyle benzerlik göstermektedir.

[37] Türk Dil Kurumu, *Güncel Türk Sözlük*, https://sozluk.gov.tr/, (11.12.2019).

[38] TÜBA, *Türkçe Bilim Terimleri Sözlüğü*, http://www.tubaterim.gov.tr/, (11.12.2019).

[39] Akbulut, s.353.

[40] Dülger, s. 457; Akbulut, s.353;

[41] Akbulut, s.353; Korkmaz, s.51.

güvenlik kodlarının suçun konusu olarak kabul edildiğini izah etmesinin yerinde olacağı tespitini de içermektedir[42]. Öte yandan bir başka görüş, sistem tarafından üretilen algoritmalar olan güvenlik kodlarına farklı isimler verilebildiği, bu nedenle kanun koyucunun isimleri farklı olsa da tüm kodları kapsam içine almak üzere bu ifadeyi kullanmayı tercih ettiğidir[43]. Aktarılan iki görüş bakımından yapılan iki tespite de katılmaktayız. Bu bağlamda kanımızca sisteme giriş yapılmasına imkan sağlayan kodlara farklı isimler verilebildiği, isim farklılığı nedeniyle bir düzenleme boşluğu doğabileceği gözetildiğinde sair güvenlik kodu ifadesinin TCK'nın 245/A maddesinde muhafazası gereklidir. Yukarıda ortaya konulduğu üzere 245/A maddesinde kullanılan şifre ifadesinin önüne "bir bilişim sisteminin tamamına ya da bir kısmına erişimi mümkün kılan" nitelendirmesinin eklenerek hükmünün yeniden formüle edilmesinin sair güvenlik kodları açısından da belirsizliği gideren bir çözüm olabileceği görüşündeyiz.

(5) Münhasıran Bilişim Alanında İşlenen Suçlar veya Bilişim Sistemleri Aracılığıyla İşlenebilen Diğer Suçların İşlenmesinde Kullanılmak Üzere Yapılmış ya da Oluşturulmuş Olmak Koşulu

Her cihaz, bilgisayar programı, şifre veya güvenlik kodu TCK'nın 245/A maddesinde düzenlenen suçun maddi konusunu teşkil etmez. Çünkü TCK'nın 245/A maddesinde, bilgisayar programı, şifre veya güvenlik kodunun ya münhasıran bilişim alanında işlenen suçların veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesi için yapılması ya da farklı bir amaçla yapılmış olmakla birlikte söz konusu suçları işlemeye yönelik sonradan uyarlanmış olması aranarak suçun maddi konusu sınırlandırmaya çalışmıştır. Bu tespitin dayanağı TCK'nın 245/A maddesinde "*..münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda..*" şeklinde yer verilen ifadedir.

Aktarılan düzenlemenin isabetli olmadığı görüşündeyiz. Çünkü öncelikle 245/A maddesinde kullanılan "*bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen bir suç*" ifadesinin anlamsal sınırlarını tespit etmek güçtür[44]. İfadenin geniş yorumlanması halinde bilişim sistemlerinin hayatlarımızdaki yeri ve bilişim teknolojisindeki gelişmelerin hızı dikkate alındığında tüm suç tiplerinin bilişim sistemleri kullanılmak suretiyle işlenebileceği sonucuna ulaşılabilir ki bu

---

42 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1031.

43 Akbulut, s.353.

44 TCK'nın 245/A maddesi hükmünün bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçların hangi suçlar olduğu açık olarak ifade edilmediğinden kanunilik ilkesiyle çeliştiği tespiti için bkz. Korkmaz, s.52.

yorum TCK'nın 245/A maddesinin kanunilik ilkesiyle ve özellikle de belirlilik esasıyla çelişen şekilde uygulanmasına yol açacaktır. Kanımızca aktarılan ifadeyi dar yorumlamak, sadece bilişim sistemlerinin kullanılması suretiyle işlenmeleri suçun nitelikli hali sayılan suçlar[45] ile sınırlı olarak anlamlandırmak yerinde olacaktır[46]. Olması gereken hukuk açısından değerlendirme yapmak bakımından Siber Suç Sözleşmesi'nin 6. fıkrasında sadece yasadışı erişim, yasadışı müdahale, verilere müdahale ve sisteme müdahale fiillerini gerçekleştirmek amacıyla gerçekleştirilen fiiller bakımından taraf devletler için suç haline getirme yükümlülüğü öngörüldüğü vurgulanmalıdır.

TCK'nın 245/A maddesinde yer alan "..*münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda*.." ifadesinin isabetli olmadığı tespitinin dayandığı ikinci neden, hükmün suç işlemek için yapılmayan veya oluşturulmayan programlar ile ilgili olarak uygulanma kabiliyetinin bulunmamasıdır. Örneğin bilişim sistemlerinin güvenliğinin test edilmesi için gerçekleştirilen sızma testlerinde kullanılmak üzere geliştirilen bir program, Bilişim Alanında Suçlar Bölümünde yer alan suçların işlenmesinde kullanılmak amacıyla satın alınırsa suçun maddi konusunun yokluğu nedeniyle tipe uygunluk unsuru gerçekleşmeyecektir. Çünkü bu nitelikte bir program münhasıran bilişim alanında suçların veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesinde kullanılmak üzere yapılmış ya da oluşturulmuş değildir. Bu sonuç suçla korunan hukuki değerlerle bağdaşmasa da aksi sonuca varmak ancak kıyasa yapmak ile mümkün olabilir ki bu suçta ve cezada kanunilik ilkesiyle çelişecektir.

Kanımızca çözüm TCK'nın 245/A maddesinin Siber Suç Sözleşmesinin 6. maddesi hükmünde olduğu gibi tipe uygun davranışın sınırlandırılarak ve hukuka uygun amaçlarla oluşturulmuş olan programlarının bilişim alanında suçların işlenmesine hazırlık olması amacıyla el değiştirmesine yönelik fiilleri de kapsayacak şekilde yeniden formüle edilmesidir[47].

---

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

[46] Öğretide Gül aksi kanaatte olup, tehdit, hakaret, şantaj, hırsızlık, dolandırıcılık, zimmet, sahtecilik, haberleşmenin gizliliğini ihlal, kişisel verilerin kaydedilmesi, suç işlemeye tahrik, halkı kin ve düşmanlığa tahrik, müstehcenlik, kumar oynanması için yer ve imkan sağlama, devlet sırlarının ifşası, fikri hakların ihlali gibi çok sayıda suçun bilişim sistemi aracılığıyla işlenmesinin mümkün olduğunu, bu suçların gerçekleştirilmesine yönelik olarak cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun sağlanmasına yönelik olarak gerçekleştirilen fiillerle TCK'nın 245/A maddesinde düzenlenen suçun oluşmasının mümkün olduğunu savunmaktadır. Bkz. Gül, s. 242.

[47] Örneğin Alman Ceza Kanunu'nun 202/c maddesinde sadece veri casusluğu veya verileri iletirken ele geçirme suçlarının (Alman Ceza Kanunu'nun 202a veya 202b maddelerinde

c. Eylem

TCK'nın 245/A maddesinde tipe uygun eylem; imal etmek, ithal etmek, sevk etmek, nakletmek, depolamak, kabul etmek, satmak, satışa arz etmek, satın almak, başkasına vermek veya bulundurmak[48] hareketleri seçimlik olarak sıralanmak suretiyle tanımlanmıştır[49]. Bu sebeple suçun oluşması bakımından TCK'nın 245/A maddesinde sayılan seçimlik hareketlerden yalnızca birinin gerçekleştirilmesi yeterlidir. Yine aynı nedenle suçun konusunun ortak olması şartıyla TCK'nın 245/A maddesinde sıralanan hareketlerden birden çoğunun gerçekleştirilmesi halinde tek bir suçun işlendiği sonucuna varmak gerekir[50].

Aşağıda TCK'nın 245/A maddesinde yer alan seçimlik hareketler kısaca incelenecek olup, daha sonra bu hareketlerle bağlantı olan suçun yapısal özellikleri belirlenmeye çalışılacaktır.

İmal etmek, üretmek anlamına gelmektedir. Mevcut bir cihazın ya da programın bazı değişiklikler yapılmak suretiyle yeni bir içeriğe ya da işleve sahip hale getirilmesi de bu hareketin kapsamında değerlendirilmelidir. Örneğin mevcut bir program açısından yazılımın türevinin geliştirilmesi ana yazılımdan ayırt edilebilir birtakım özelliklere sahip olması şartıyla üretme olarak nitelendirilebilir[51]. İmal hareketinin tamamlanması bakımından henüz kablolarından bir kısmının takılmaması gibi cüzi tamamlama ihtiyacının bulunmasının önem taşımadığı belirtilmelidir[52].

düzenlenen suçların) işlenmesini hazırlamak amacıyla Alman Ceza Kanunu'nun 202a maddesinin 2. fıkrası kapsamında verilere giriş yapmayı sağlayan şifre veya güvenlik kodlarının, ya da bu tür fiilleri işlemeyi amaçlayan bilgisayar programlarının üretimi, kişinin kendisine ya da bir başkasına tedariki, satışı, yayma ya da ulaşılabilir hale getirilmesi fiilleri suç haline getirmiştir. Bu suç tipine ilişkin bkz. Gunther Arzt, Ulrich Weber, Bernd Heinrich ve Eric Hilgendorf, *Strafrecht Besonderer Teil*, Bielefeld 2009, s.247 vd; Jörg Eisele, *Strafrecht - Besonderer Teil I,* Stuttgart 2012, s.245 vd.

48 Öğretide ileri sürülen bir görüşe göre bu seçimlik hareketleri arasında yayma fiiline yer verilmemesi eleştirilmeye değerdir. Suçun yayma hareketini de kapsayacak şekilde düzenlenmesi suçla mücadele bakımından bir gereklilik olarak nitelendirilebilir. Bkz. Akbulut, s. 357; Aynı yönde bkz. Korkmaz, s.52; Öğretide Dülger'e göre yayma fiiline TCK'nın 245/A maddesinde yer verilmemiş olması diğer seçimlik hareketler dikkate alındığında büyük bir boşluk oluşturmamaktadır. Bkz. Dülger, s.457; Bu tartışma açısından öncelikle Siber Suç Sözleşmesi'nin 6. maddesinde de taraf devletler için suç haline getirme yükümlülüğü öngörülürken yayma fiiline de yer verildiğine dikkat çekmek istemekteyiz. Ancak TCK'nın 245/A maddesinde tipikleştirilen fiiller göz önünde bulundurulduğunda yayma kapsamında değerlendirilebilecek eylemlerim ekseriyetle satmak, nakletmek, sevk etmek, vermek suretiyle işlenebileceği düşüncesindeyiz. İfade edilen nedenle aktardığımız son görüşe katılmaktayız.

49 Suçun seçimlik hareketli bir suç olduğu tespiti için bkz. Dülger, s.457; Gül, s.240; Akbulut, s.355; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s.914; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1031 vd; Korkmaz, s.51.

50 Akbulut, s.355; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s.914; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1032; Korkmaz, s.51.

51 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1032; Akbulut, s.355.

52 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1032; Akbulut, s.355.

İthal etmek, yurt dışından yurt içine getirmeyi anlatır. Bir bilgisayar programının, şifrenin veya güvenlik kodunun internet üzerinden ülkeye sokulması da ithal hareketi kapsamında değerlendirilmelidir[53]. Öte yandan TCK'nın 245/A maddesinde suç tanımında ithal hareketine yer verilmesine rağmen ihraç hareketine yer verilmediği görülmektedir. Kanun koyucunun bu tercihi, TCK'nın 245/A maddesinde satın almak hareketinin de tipik hareket olması sebebiyle bir düzenleme boşluğu oluşturmamaktadır[54].

Sevk etmek göndermeyi ifade eder. Öğretide ileri sürülen bir görüşe göre nakletmek de aynı ya da yakın anlama geldiğinden TCK'nın 245/A maddesinde her iki fiile de yer verilmesi isabetli olmamıştır[55]. Öğretide aktarılan tespitin depolamak ve bulundurmak fiilleri açısından da tekrarlandığı görülmektedir[56]. Söz konusu tespitin dayanağı depolamanın saklamak veya korumak amacıyla biriktirmeyi veya bir bellek cihazına veriyi yerleştirmeyi ya da saklamayı ifade etmesi, bulundurmanın bir şeyin var olmasını, hazır bulunmasını sağlamayı anlatmasıdır ki suçun maddi konusu düşünüldüğünde her iki hareket arasında anlamsal bir yakınlık olduğu görülmektedir. Ancak bu yakınlığa rağmen bulundurmak ve depolamak arasında ince bir çizginin bulunduğu da örtülü olarak öğretide ifade edilen bir başka görüştür. Çünkü yazılımlar bakımından ortaya konulan bu görüşe göre her kayıt depolama değildir. Dijital ortamda her türlü bulundurma (depolama ya da depolama olmaksızın geçici kullanım) bir tür kayıt altına almadır. Depolama için yapılan kaydın niteliği, boyutu ve amacı gibi unsurlar göz önünde bulundurulmalıdır[57].

Kabul etmek, bedelsiz olarak verilen cihazın, bilgisayar programının, şifrenin ya da güvenlik kodunun alınmasını anlatmaktadır[58]. Kabulün sürekli ya da geçici süreli oluşu, söz gelimi cihazın iade edilecek olması, kabul hareketinin oluşması ve tamamlanması açısından önem taşımamaktadır.

Satmak, satıcının bir bedel ödenmesini üstlenmesi karşılığında alıcıya suçun konusu olan cihaz, bilgisayar programı, şifre ya da güvenlik kodunu vermesini ya da sağlamasını ifade eder. Bu hareketin tamamlanması bakımından satılan

---

53 Korkmaz, s.51; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1032; Akbulut, s.355.

54 İhraç fiiline yer verilmese de bu ihraç niteliğindeki eylemlerin sevk etmek veya nakletmek kapsamında olacağı tespiti için bkz. Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1033; Akbulut, s.356; Sevk etmek ve nakletmek suçun diğer seçimlik hareketleri olduğu için ihraç fiiline TCK'nın 245/A maddesinde yer verilmemesinin bir boşluk yaratmadığı görüşü için bkz. Korkmaz, s.52.

55 Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s.914; Sevk etme eyleminde üçüncü kişinin aracılığının söz konusu olduğu, nakletmek eyleminin fail tarafından gerçekleştirildiği, bu sebeple sevk etmek ve nakletmek eylemlerinin farklı anlamlara geldiğine ilişkin aksi yöndeki görüş için bkz. Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1033; Korkmaz, s.52.

56 Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s.914.

57 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1033.

58 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1033; Akbulut, s.356.

cihaz, bilgisayar programı, şifre ya da güvenlik kodunun karşılığı teşkil eden bedelin fiili olarak verilmiş ya da sağlanmış olması önem taşımamaktadır[59].

Satışa arz ise cihaz, bilgisayar programı, şifre ya da güvenlik kodunun bedel karşılığı satılması iradesini ortaya koyacak şekilde satışa sunulmasını anlatır. Bu eylemin gerçekleşmesi bakımından somut bir alıcının bulunması gerekmemektedir. Kanun koyucunun TCK'nın 245/A maddesinde satmak eyleminin yanı sıra satışa arz etmek eylemine de yer vererek satmak eylemi bakımından suç yolunda teşebbüs aşamasında kalacak davranışların da suçun tamamlanmış cezası ile cezalandırılmasını sağlamayı uygun gördüğü söylenebilir. Bu tercih Siber Suç Sözleşmesinin 6. maddesinde taraf devletler için öngörülen suç haline getirme yükümlülüğünün kapsamını aşmaktadır. Kanımızca düzenlemenin orantılılık ilkesinin bir alt unsuru olan ceza hukukunun ikincillik ilkesiyle bağdaşmadığı yönünde eleştirilmesi mümkündür.

Satın almak, bedel karşılığında suçun konusu olan cihaz, bilgisayar programı, şifre ya da güvenlik kodunu temini ya da erişim imkanın elde edilmesidir. Bu hareketin tamamlanması bakımından bedelin karşı tarafa ulaştırılmasının ya da satın alınan cihazın veya program, şifre ya da güvenlik kodunun teslim edilmiş ya da erişimin sağlanmış olmasının gerekmediği vurgulanmalıdır. Bir diğer ifade ile bir satıcı ile satış sözleşmesinin yapılmış olması hareketin gerçekleşmesi bakımından yeterlidir.

Öte yandan yukarıda belirtildiği üzere TCK'nın 245/A maddesinde satmanın yanı sıra satışa arz etme hareketi de sayılmışken suç yolunda satın alma hareketinden önce gerçekleştirilmesi ihtimal dâhinde bulunan somut bir satıcı ya da genele yönelen satın alma iradesini ortaya koyan davranışların tipikleştirilmemesi dikkat çekicidir. Bu farklılık özellikle teşebbüs bakımından işlevseldir.

Başkasına vermek ise satış niteliği olmaksızın cihazın, bilgisayar programını, şifre veya sair güvenlik kodunun teslim edilmesini anlatır. Kanun koyucu bedel karşılığı olmayan temin fiillerinin cezalandırılmasında boşluk doğmaması için bu harekete de TCK'nın 245/A maddesinde yer vermeyi uygun bulmuştur.

Yukarıda kısaca açıklamaya çalıştığımız TCK'nın 245/A maddesinde yer alan seçimlik hareketler yönünden suç tipinin özelliklerini saptamak gerekirse yapılabilecek ilk tespit, TCK'nın 245/A maddesinde eylemin gerçekleştirilme tarzına yönelik sınırlayıcı nitelendirmelere yer verilmediğinden suçun serbest hareketli bir suç olduğudur[60].

---

[59] Kaldı ki bir an için aksi kabul edilse bile TCK'nın 245/A maddesinde seçimlik hareketler arasında satışa arz etmek de ayrıca yer almaktadır. Bu sebeple bilgisayar programı, şifre ya da güvenlik kodunun karşılığı teşkil eden bedelin henüz alınmamış olması halinde satışa arz aşaması geçilmiş olacağı için eylem tamamlanmış olacaktır.

[60] Gül, s.240 vd; Suçun bağlı hareketli bir suç olduğuna ilişkin aksi yönde görüş için bkz. Akbulut, s.355; Korkmaz, s.51.

İkinci tespit, suçun bulundurma ve depolama eylemleri yönünden söz konusu hareketlerin yapısal olarak icralarının devam eden özellik göstermesi sebebiyle kesintisiz suç teşkil ettiği, diğer hareketler bakımından ise bu özellik bulunmadığından suçun ani suç vasfı taşıdığıdır[61]. Belirtilen tespit özellikle iki açıdan önemlidir. İlki suçun işlendiği yer ve zamanın belirlenmesidir[62]. Çünkü kesintisiz suçlarda suç hareketin icrasının başladığı yerde ve zamanda değil, kesintinin gerçekleştiği yer ve zamanda işlenmiştir. Bu tespitin önem taşıdığı ikinci husus iştirak olup, söz konusu hareketler bakımından suça iştirak kesintinin gerçekleştiği ana kadar mümkündür.

Yapılabilecek üçüncü tespit suçun sırf hareket suçu vasfı taşıdığıdır[63]. Çünkü TCK'nın 245/A maddesinde suçun oluşması bakımından yukarıda incelenen hareketlerin gerçekleştirilmesi yeterli kabul edilmiş, bu hareketlerle nedensellik bağı içinde gerçekleşmesi gereken bir netice aranmamıştır.

Yapılabilecek son tespit ise suçun soyut tehlike suçu vasfı taşıdığıdır[64].

2. Subjektif Nitelikteki Unsurlar

TCK'nın 245/A maddesinde düzenlenen suçun tipe uygunluk unsuru içinde yer alan sübjektif hususlardan ilki kasttır. Bu diğer ifade ile bu suç ancak kasten işlenebilir. Çünkü TCK'nın 245/A maddesinde tarif edilen fiilin taksirle işlenmesi halinde faile ceza verileceğine ilişkin özel bir düzenleme bulunmamaktadır.

Suçun tipe uygunluk unsuru içinde yer alan diğer sübjektif husus ise özel kast olup, failin cihaz, bilgisayar programı, şifre ve sair güvenlik kodunu imal etme, ithal etme, sevk etme, nakletme, depolama, kabul etme, satma, satışa arz etme, satın alma, başkalarına verme veya bulundurma fiilini TCK'nın Bilişim Alanında İşlenen Suçlar Bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen başka bir suçun işlenmesinde faydalanmak veya faydalanılması amacıyla gerçekleştirmesi gerekir[65].

Bu tespite dayanak olarak TCK'nın 245/A maddesinde yer alan "*TCK'nın Bilişim Alanında İşlenen Suçlar Bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması ya da oluşturulması durumunda*" ifadesi gösterilebilir. İfade edilen görüş, Türkiye'nin de tarafı olduğu Siber Suç Sözleşmesinin 6. maddesindeki düzenleme

---

61 Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s.914; Dülger, s.458; Akbulut, s.355.

62 Suçun işlendiği zaman ve zamanaşımının başlangıcı bakımından bu tespit için bkz. Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s.914; Zaman bakımından uygulanacak kanunun tespiti ve zamanaşımının başlangıcı ile mahkemelerin yer bakımından yetkisi bakımından bu tespit için bkz. Dülger, s.458.

63 Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s.915; Dülger, s.458; Akbulut, s.355; Korkmaz, s.51.

64 Akbulut, s.355; Korkmaz, s.51; Dülger, s.458.

65 Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.915; Dülger, s.458.

ile de örtüşmektedir[66]. Çünkü Siber Suç Sözleşmesinin 6. maddesinde taraf devletler için Sözleşmenin 2 ila 5. maddelerinde tanımlanan yasa dışı erişim, yasa dışı araya girme, verilere müdahale fiillerinin[67] gerçekleştirilmesinde kullanılmaları amacıyla bir bilgisayarın tamamına veya herhangi bir kısmına erişimi mümkün kılan bilgisayar şifresi, erişim kodu veya benzeri bir verinin ya da söz konusu fiilleri işlemek amacıyla bilgisayar programı dahil tasarlanmış veya uyarlanmış cihazın üretimini, satışını, kullanım amaçlı tedarikini, ithalini, dağıtımını veya başka şekilde erişilebilir hale getirilmesini suç haline getirme yükümlülüğü öngörmüştür. Fakat aynı zamanda Sözleşmenin 6. maddesinde taraf devletler için suç haline getirme yükümlülüğünün Sözleşmenin 2 ila 5. maddelerinde tanımlanan yasa dışı erişim, yasa dışı araya girme, verilere müdahale fiillerinin işlenmesinde faydalanmak amacıyla değil de örneğin bir bilgisayar sisteminin yetkililerce test edilmesi gibi başka bir amaçla gerçekleştirilmesi halini kapsamayacağı da belirtilmiştir. Bu hüküm düzenleniş biçimi nedeniyle iç hukukta doğrudan uygulanabilir değildir. Dolayısıyla Anayasanın 90. maddesinin son fıkrasının son cümlesi kapsamında kaynak değeri taşımamaktadır. Ancak yine de belirtilen Sözleşme hükmünden daraltıcı yorum yapmak üzere yararlanmak mümkündür.

Bir an için TCK'nın 245/A maddesinde yer alan suçun oluşması bakımından kastın yeterli olduğu, failin taşıması gereken özel bir saik aranmadığı ve hükümde yer alan "*TCK'nın Bilişim Alanında İşlenen Suçlar Bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması ya da oluşturulması durumunda*" ifadesinin sadece suçun maddi konusunu nitelendirmek için kullanıldığı kabul edilirse, TCK'nın 245/A maddesi ile sızma testi[68] gerçekleştirmek gibi farklı amaçlarla bulundurulması olasılık dahilinde olan pek çok yazılımın yasaklandığını söylemek gerekecektir. Bu sonucun suçla korunan hukuki değere bizzat zarar vereceği, kusursuz suç olmaz prensibi ile çelişen uygulamalalara neden olacağı ve Anayasa'nın 17. maddesinde yer alan kişinin maddi ve manevi varlığını geliştirme hakkıyla bağdaşmayacağı ortadadır.

---

66 Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.915.

67 Hukukumuzda bu fiiller yukarıda incelediğimiz TCK'nın 243 ve 244. maddelerinde tipikleştirilmiştir.

68 Sızma testi, kötü amaçlı bir saldırganın sisteme verebileceği hasarları raporlamak ve bu hasarlara yönelik olarak önceden savunma tedbirleri almak maksadıyla bir kurumun bilişim sistemlerinde güvenlik açıklarının bulunması konusunda yetkilendirilmiş kişiler tarafından yapılan testlerin tamamına denilmektedir. Kavram için bkz. Alisherov A Farkhod ve Sattarova Y Feruza, "Methodology For Penetration Testing", *International Journal of Grid and Distributed Computing*, Vol.2, No.2, June 2009, s.43; Andrew Tang, "A Guide To Penetration Testing", *Network Security*, Vol. 2014, Iss. 8, August 2014, s.8; Mustafa Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, İstanbul 2018, s.2 vd; Çıtak, s.8.

Kanımızca TCK'nın 245/A maddesinin belirtilen şekilde yorumlanması halinde doğabilecek sıkıntıların bertaraf edilmesi için en isabetli çözüm TCK'nın 245/A maddesinde kanun koyucu tarafından bir değişikliğe gidilmesidir. Söz konusu hükümde yer alan "..*bilişim alanında işlenen suçlar bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması ya da oluşturulması durumunda*" ifadesinin kaldırılarak hükmün "…*TCK'nın bilişim alanında işlenen suçlar bölümünde düzenlenen suçlarının işlenmesi için hazırlık yapılması amacıyla*" ifadesinin kullanılmak suretiyle yeniden formüle edilmesi bir öneri olarak değerlendirilebilir[69].

Öte yandan TCK'nın 245/A maddesinde düzenlenen suç bakımından failin özel bir saikle hareket etmesi gerektiğinden suçu olası kast ile işlenmesi mümkün değildir[70].

B. Hukuka Aykırılık Unsuru

Bilişim suçlarının işlenmesi amacıyla cihaz, program, şifre veya güvenlik kodlarının üretilmesi, yayılması ya da bulundurulması suçunun tipe uygunluk unsuru dikkate alındığında meşru savunma hukuka uygunluk nedenin uygulanmasının bu suç bakımından mümkün olmadığı anlaşılmaktadır[71]. Çünkü suçun tipe uygunluk unsuru kapsamında yer alan fiiller, mevcut bir haksız saldırıyı bertaraf etmeye yönelik saldırgana karşı gerçekleştirilen bir savunma hareketi ile ilişkilendirilebilir değildir.

Hakkın kullanılması hukuka uygunluk nedenin de bu suç bakımından uygulama alanı bulması mümkün değildir. Çünkü failin TCK'nın Bilişim Alanında İşlenen Suçlar Bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen başka bir suçun işlenmesinde faydalanmak veya faydalanılması amacıyla hareket ederken aynı zamanda sübjektif bir hakkı kendi içkin sınırları içinde kullandığı sonucuna ulaşmak olası gözükmemektedir.

Yine TCK'nın 245/A maddesi bakımından ilgilinin rızası, hukuka uygunluk nedeni teşkil etmeyecektir[72]. Çünkü bu suçun mağduru yukarıda incelendiği üzere belli bir kişi olmayıp toplumdur.

---

69 Bu öneriye ilişkin olarak pek çok olayda failin kastının belirlenmesinde güçlük yaşanabileceği ve şüpheden sanık yararlanır ilkesi gereğince beraat kararı verilmesi gerekeceği eleştirisi yapılabilirse de kanımızca bu haklı tespit teşebbüs suçlarının hepsi açısından tekrarlanabilir niteliktedir. Söz konusu önerinin belirtilen eleştirilere maruz kalmaması için bir çözüm önerisi olarak karşılaştırmalı hukukta da örnekleri bulunduğu üzere suçun konusu bakımından sayı şartı fikri geliştirilebilir. Bkz. 21. nolu dipnottaki açıklamalar

70 Dülger, s.458; Aksi yönde bkz. Akbulut, s.358; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1034.

71 Akbulut, s.358.

72 Akbulut, s.358; Aksi yönde bkz. Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1034; Korkmaz, s.53.

Son olarak öğretide ileri sürülen CMK'nın 134. maddesinde düzenlenen bilgisayarda, bilgisayar programında, bilgisayar kütüğünde arama, kopyalama ve elkoyma koruma tedbirinin uygulanmasına yönelik olarak cihaz, program, şifre ya da kodun bulundurulması veya depolanması halinde kanun hükmünün yerine getirilmesi hukuka uygunluk nedenin oluşacağına ilişkin görüşe dikkat çekmek istemekteyiz[73]. Aktardığımız görüşe katılmamaktayız. Kanımızca belirtilen durumda suçun oluşmama nedeni tipe uygunluk unsurunun gerçeklememesidir. Çünkü bu durumda CMK'nın 134. maddesi kapsamında koruma tedbirinin icrası kapsamında kullanmak üzere cihaz, program ya da şifre veya sair güvenlik kodu bulundurulmaktaysa failin TCK'nın Bilişim Alanında İşlenen Suçlar Bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen başka bir suçun işlenmesinde faydalanmak veya faydalanılması amacıyla hareket ettiğini söylemek mümkün değildir. Aktarılan nedenle bu olasılıkta hukuka uygunluk nedenleri açısından bir tartışma yapmaya gerek bulunmadığı kanaatindeyiz.

C. Kusurluluk Unsuru

Kusurluluk; failin hukuka uygun hareket edebilme imkanına sahip olmasına karşın hukuka aykırı bir davranışı seçmiş ve gerçekleştirmiş olması nedeniyle kınanabilmesi ve neticenin ona sübjektif olarak yüklenebilmesini anlatır[74]. Suçun kusurluluk unsurunun oluştuğu sonucuna varmak için öncelikle failin kusur yeteneğine sahip olması gerekir. Bu koşulun gerçekleşip gerçekleşmediği belirlenirken somut olayda kusur yeteneğine etki eden nedenlerin (yaş küçüklüğü, akıl hastalığı, sağır ve dilsizlik, geçici nedenler ile alkol veya uyuşturucu madde etkisi altında olma) bulunup bulunmadığı saptanmalıdır. İfade edilen husus açısından TCK'nın 245/A maddesi bir özellik göstermemekte olup, genel esaslar geçerlidir.

Kusurluluğun diğer koşulu, somut olayda kusurluluğu kaldıran bir nedenin gerçekleşmemesidir. Kusurluluğu kaldıran nedenler açısından TCK'nın 245/A maddesindeki suç açısından cebir- şiddet- tehdide ilişkin TCK'nın 28. maddesinin uygulama alanı bulabileceği söylenebilir.

---

73 CMK'nın 134. maddesinde öngörülen koruma tedbirini kanun hükmünün yerine getirilmesi hukuka uygunluk nedeni ile ilişkili olarak değerlendiren görüş için bkz. Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1034; Korkmaz, s.53; CMK'nın 134. maddesinde öngörülen koruma tedbirini görevin ifası hukuka uygunluk nedeni ile ilişkili olarak değerlendiren görüş için bkz. Akbulut, s.359; genel olarak CMK'nın 134. maddesinde öngörülen koruma tedbirine başvurulmasına yönelik gerçekleştirilen fiillerin hukuka uygun olduğu tespiti için bkz. Dülger, s.459.

74 Kusurluluğun anlamı için bkz. Bahri Öztürk ve Mustafa Ruhan Erdem, *Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri*,19. Baskı, Ankara 2019, s.308 vd; Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, 10. Baskı, Ankara 2019, s.346 vd; İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler*, 14. Baskı, Ankara 2018, s.390 vd; Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, 12. Baskı, Ankara 2019, s.309 vd.

Buna karşılık kanımızca bir diğer mazeret sebebi olan zorunluluk haline ilişkin TCK'nın 25. maddesinin 2. fıkrası hükmünün zorunluluk halinin koşulları dikkate alındığında inceleme konumuzu oluşturan suç bakımından uygulanması mümkün gözükmemektedir. Çünkü zorunluluk halinin oluşabilmesi için varlığı gereken koşullar arasında kişinin bilerek neden olmadığı ağır ve muhakkak bir tehlikeden başka türlü korunma imkanın bulunmaması koşulu da yer almaktadır. Kanımızca TCK'nın 245/A maddesiyle tanımlanan seçimlik hareketler dikkate alındığında belirtilen koşulun oluşması olanaksızdır.

Kusurluluğu kaldıran hallerden bir diğeri, TCK'nın 30. maddesinin 4. fıkrasında düzenlenen yasaklılık yanılmasıdır. TCK'nın 245/A maddesinde düzenlenen suçun oluşması bakımından failin taşıması gereken amaç dikkate alındığında failin tipe uygun davranışı gerçekleştirmesine rağmen kaçılmaz olarak haksızlık bilincinden yoksun olduğunu söylemek mümkün değildir. İfade edilen nedenle inceleme konumuzu oluşturan suç açısından TCK'nın 30. maddesinin 4. fıkrasının uygulanma ihtimali bulunmadığı kanaatindeyiz.

Kusurluluğu kaldıran hallerden sonuncusu amirin hukuka aykırı emridir. TCK'nın 245/A maddesinde düzenlenen suç bakımından bu nedene dayalı olarak suçun kusurluluk unsurunun oluşmadığı sonucuna varılamayacağını düşünmekteyiz. Çünkü TCK'nın 24. maddesinin 2 vd. fıkralarıyla Anayasa'nın 137. maddesindeki düzenleme nedeniyle amirin hukuka aykırı emrinin yerine getirilmesinin kusurluluğa etki edebilmesi için öncelikle emrin konusunun suç teşkil etmemesi gerekir. Bu bakımdan eğer fail TCK'nın Bilişim Alanında İşlenen Suçlar Bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen başka bir suçun işlenmesinde faydalanmak veya faydalanılması amacıyla cihaz, program, şifre ya da kodun bulundurulması veya depolanması ya da TCK'nın 245/A maddesinde sıralanan diğer hareketlerden birini yapmasına yönelik olarak emir almış ve yerine getirmiş ise konusu suç teşkil eden bir emri yerine getirmiş demektir. Bu durumda emrin yazılı olarak tekrarlanması onun sorumluluğu ortadan kaldırmamaktadır. Fail emrin TCK'nın Bilişim Alanında İşlenen Suçlar Bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen başka bir suçun işlenmesinde faydalanılması amacıyla hareket etmemiş ise kusurluluğu kaldıran bir neden olarak amirin hukuka aykırı emrini tartışmaya gerek yoktur. Çünkü zaten belirtilen olasılıkta fiil tipe uygun olmayacaktır.

IV. TEŞEBBÜS

Öğretide sırf hareket suçu olması sebebiyle TCK'nın 245/A maddesinde düzenlenen suç açısından icra hareketlerinin parçalara bölünebilmesi halinde teşebbüs hükümlerinin uygulanacağı ifade edilmektedir[75]. Örneğin bilişim

[75] Akbulut, s.359 vd; Dülger, s.459; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1035; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.915; Korkmaz, s.53.

alanında suç işlemekte kullanılmak üzere bir cihazın imaline başlanmış ancak polis baskını yapılması nedeniyle imalat tamamlanamamış ise teşebbüs hükümlerinin uygulanması gerekecektir[76].

İnceleme konumuzu oluşturan suçun teşebbüse elverişli olduğu yönündeki yukarıda aktardığımız tespite söz konusu suçun tipe uygunluk unsuru içinde yer alan satma ve satışa arz eylemleri dışında katılmaktayız. Çünkü satışa arz, satış eyleminin suç yolunda teşebbüs aşamasında yer alan parçası olarak değerlendirilebilir. Kanun koyucu bu hareketi tamamlanmış suç gibi cezalandırmak istemiş, bu sebeple de suç tipinde belirtilen harekete suçun seçimlik hareketi olarak yer vermeyi uygun görmüştür. Bir diğer ifade ile satışa arz hareketi açısından suçun, tamamlanması öne alınmış suç (teşebbüs suçu) vasfı taşıdığı söylenebilir. Kanun koyucunun bu tercihi nedeniyle teşebbüs açısından iki sonuca varmak mümkündür. Bunlardan ilki satışa arz hareketinin teşebbüse elverişli olmadığıdır[77]. İkincisi, satma eylemi bakımından suç yolunda teşebbüs aşamasında değerlendirilmesi gereken hareketler zaten satışa arz eylemini oluşturacağından satma hareketi açısından suçun teşebbüse elverişli olmadığıdır.

V. İŞTİRAK

Bilişim alanında suçların veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre ya da güvenlik kodlarının üretilmesi, yayılması veya bulundurulması suçu bakımından iştirak, satma - satın alma, başkasına verme - kabul etme, ithal etme - satma eylemleri açısından özellik gösterir. Çünkü bu eylemler, çok failli suçların karşılaşma suçları denilen birden fazla failin hareketlerinin ortak amaca ulaşmak üzere zıt istikamette gerçekleşmesi suretiyle işlenen türü[78] kapsamında değerlendirilmelidir[79]. Dolayısıyla satan - satın alan, başkasına veren - kabul eden, ithal eden satan kişi, suça yardım eden veya azmettiren sıfatıyla suça iştirak eden konumunda değil, fail konumundadır.

İştirak bakımından ayrıca kusurluluğu ortadan kaldıran hallerden cebir - şiddet veya tehdit durumunun söz konusu olması halinde cebir - şiddet veya tehdit uygulayarak bir başkasını bilişim alanında suçların veya bilişim

---

[76] Akbulut, s. 360; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.915; Dülger, s.459; Korkmaz, s.53.

[77] Teşebbüs suçu ve teşebbüs suçlarının teşebbüsün cezalandırılmayacağına ilişin bkz. Koca/Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s.433; Özgenç, s.507; Önder Tozman, *Suça Teşebbüs*, Ankara 2015, s. 228.

[78] Karşılaşma suçları için bkz. Sancar, s.120 vd; Demirbaş, s.498; Koca/Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s.445; Özgenç, s.519; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, s.506; Öztürk ve Erdem, s.402.

[79] Suçun bazı seçimlik fiiller bakımından çok failli suç özelliği taşıdığı yönünde bkz. Akbulut, s.350; Dülger, s.456; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.913; Korkmaz, s.49.

sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre ya da güvenlik kodlarının üretilmesi, yayılması veya bulundurulması suçunu işlemeye zorlayanın TCK'nin 28. maddesine göre dolaylı fail olacağına dikkat çekmek gerekir.

Son olarak inceleme konumuz olan suç bakımından azmettirme ve yardım eden sıfatıyla suça iştirakın mümkün olduğu ancak TCK'nın 245/A maddesinde düzenlenen seçimlik hareketlerin çeşitliliği dikkate alındığında bu suç bakımından azmettirme ile yardım edene ilişkin iştirak hükümlerinin ve bağlantılı düzenlemelerin uygulama alanının dar olacağı temel bir tespit olarak söylenebilir. Çünkü örneğin bilişim alanında suç işlemekte kullanılmak üzere üretilmiş bir programı satın alma eylemi bakımından satıcı satışa arz etmesi nedeniyle alıcıda satın alma düşüncesi ilk kez oluşturulsa bile satma eylemini gerçekleştiren fail olarak cezalandırılacak ve azmettirmeye ilişkin hükümler failiğin şerikliğe göre önceliği kuralı gereğince uygulanmayacaktır. Benzer şekilde satmak eylemi açısından nakletmek her ne kadar yardım etme niteliğinde olsa da, nakletme fiili suçun seçimlik hareketi olduğundan, nakleden kişi yardım eden olarak değil, fail olarak sorumlu tutulacaktır. Yine satan - satın alan, başkasına veren - kabul eden, ithal eden – satan kişiler azmettiren sıfatıyla katılan konumunda olmayıp suçun faili olduklarından azmettirenin belli olmaması halinde azmettirenin kim olduğunu ortaya çıkaran fail ya da suç ortağının cezasında indirim yapılabilmesine olanak sağlayan TCK'nın 38. maddesinin 3. fıkrasının inceleme konumuzu oluşturan suç bakımından uygulanması mümkünse de bu ihtimal oldukça azdır.

VI. İÇTİMA

Bilişim alanında suçların veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre ya da güvenlik kodlarının üretilmesi, yayılması veya bulundurulması suçunu işleyen fail daha sonra amaçlanan suçu işlerse her iki suçtan dolayı cezalandırılacaktır[80].

Öte yandan bu suç bakımından aynı suç işleme kararı kapsamında değişik zamanlarda birden fazla kez aynı suçun işlenmesi halinde faile tek bir suçun cezanın arttırılarak uygulanmasını öngören zincirleme suç hükmün uygulanması mümkündür[81]. Ancak zincirleme suç hükmünün uygulanması açısından özellikle salt suçun konusunun birden fazla olmasının suçun birden fazla kez işlendiği anlamına gelmeyeceğine dikkat çekilmelidir. Bir diğer ifade ile belirtilen olasılıkta suç tektir ve zincirleme suç hükmünün uygulanmaz[82].

---

[80] Akbulut, s. 360 vd; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.916; Korkmaz, s.53; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1035; Dülger, s.459 vd.

[81] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.916; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, s.1035; Dülger, s.460; Dülger, s.460; Korkmaz, s.53.

[82] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.916; Dülger, s.460; Akbulut, s.361; Korkmaz, s.53.

TCK'nın 43. maddesinin 2. fıkrasında düzenlenen aynı neviden fikri içtima hükmünün bu suç bakımından uygulanması mümkün değildir. Çünkü söz konusu düzenleme mağdurun belli birden fazla kişi olması halinde uygulanır. Oysa inceleme konumuzu oluşturan suçun mağduru belli bir kişi değil, toplumdur.

TCK'nın 44. maddesinde farklı neviden fikri içtima hükmünün uygulanması bakımından ise 136. maddede düzenlenen kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu ile TCK'nın 245/A maddesindeki ilişkiye değinmek gerekir. Çünkü TCK'nın 136. maddesinde kişisel verileri bir başkasına verme, yayma veya ele geçirme fiilleri cezalandırılmaktadır. Yukarıda incelediğimiz üzere şifreler ve sair güvenlik kodları TCK'nın 245/A maddesinde düzenlenen suçun maddi konusu içinde yer almaktadır. Dolayısıyla örneğin kişisel veri vasfı taşıyan şifreleri TCK'nın Bilişim Alanında İşlenen Suçlar bölümünde yer alan suçlardan birinde kullanılmasını sağlamak üzere satan kişi bu tek fiili ile hem TCK'nın 136. hem de TCK'nın 245/A maddesindeki suçu işlemiş olur. Bu durumda TCK'nın 44. maddesi hükmü gereği failin sadece en ağır cezayı gerektiren suçtan dolayı cezalandırılması gerekecektir. Dolayısıyla TCK'nın 136. maddesinde öngörülen ceza miktarı 245/A'da öngörülenden fazla olduğundan yalnızca TCK'nın 136. maddesinde düzenlenen suça göre cezalandırma yapılacaktır.

Görünüşte içtimaya ilişkin olmak üzere son olarak özel norm - genel norm ilişkisine işaret etmek istiyoruz. Bu bağlamda sorulması gereken temel bir soru, TCK'nın 245/A maddesinde düzenlenen suçu işleyen failin sağladığı cihaz, bilgisayar programı, şifre ve güvenlik kodu ile amaç suçun bir başkası tarafından işlenmesi halinde ayrıca bu suçtan dolayı yardım eden olarak sorumlu tutulup tutulamayacağıdır. İştirak hükümleri TCK'nın genel hükümleri arasında düzenlendiği için TCK'nın 245/A maddesi iştiraka ilişkin hükümlerle kıyaslandığında özel hüküm vasfı taşıdığından kanımızca belirtilen soruya olumsuz yanıt vermek gerekir.Öte yandan özel norm- genel norm ilişkisine dair öğretide yapılan iki tespite katılmaktayız. Yapılan ilk tespit, Elektronik İmza Kanunu'nun 16. maddesinde yer alan "*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*." hükmü ile ilgilidir. Söz konusu hüküm TCK'nın 245/A maddesine göre özel norm niteliğindedir ve dolayısıyla Elektronik İmza Kanunu'nun 16. maddesinde düzenlenen suçu işleyen faile ayrıca TCK'nın 245/A maddesine göre ceza verilmez[83] . İkinci tespit, Fikir ve Sanat Eserleri Kanunu'nun 72. maddesinde yer alan "*Bir bilgisayar programının hukuka*

[83] Dülger, s.460; Akbulut, s.361; Korkmaz, s.54.

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." hükmüyle ilgilidir. Aktarılan hüküm TCK'nın 245/A maddesine göre özel norm niteliğindedir ve bu nedenle Fikir ve Sanat Eserleri Kanunu'nun 72. maddesinde düzenlenen suçu işleyen faile TCK'nın 245/A maddesine göre değil, Fikir ve Sanat Eserleri Kanunu'nun 72. maddesine göre ceza verilmelidir[84].

VII. YAPTIRIM

Bilişim alanında suçların veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre ya da güvenlik kodlarının üretilmesi, yayılması veya bulundurulması suçunun cezası, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezasıdır. Ayrıca TCK'nın 246. maddesindeki düzenleme nedeniyle bu suç bakımından tüzel kişi aleyhine güvenlik tedbiri uygulanması mümkündür.

Suçla korunan hukuki değeri ve suç tipiyle yasaklanan davranışın özellikleri dikkate alındığında kanımızca yaptırım açısından hükmün yerinde olduğu kanaatindeyiz. Ancak son olarak bir düzenleme ihtiyacına da değinmek istemekteyiz. Kanımızca inceleme konumuzu oluşturan suç bakımından kanun koyucunun etkin pişmanlık hükmü oluşturması isabetli olacaktır. Bu bağlamda suça konu cihaz, program, şifre veya sair güvenlik kodunu kabul eden, satın alan, bulunduran veya depolayan failin soruşturma başlanmadan suçun maddi konusunu pişmanlık göstererek yetkili mercilere teslim etmesinin şahsi cezasızlık nedeni olarak düzenlenmesinin TCK'nın 245/A maddesinin amacıyla bağdaşır yararlı sonuçlar vereceği kanaatindeyiz.

SONUÇ

Uluslararası ölçeğe ulaşan hacker araçlarının kara borsasının önlenmesi, veri güvenliği ve bilişim sistemlerinin güvenliği ile güvenilirliğinin teminine ilişkin temel bir ihtiyaçtır. Türkiye'nin tarafı olduğu Siber Suç Sözleşmesinin 6. maddesi bu ihtiyacın giderilmesine ilişkin uluslararası bir mutabakatın ürünüdür. Türk kanun koyucunun söz konusu hükümden doğan suç haline getirme yükümlüğünü ifa etmek üzere TCK'nın 245/A maddesinde bilişim suçlarının ve bilişim sistemlerinin kullanılması suretiyle işlenen diğer suçların hazırlık hareketi vasfı taşıyabilecek fiilleri bağımsız suç olarak tipikleştirildiği anlaşılmaktadır.

---

[84] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s.916; Akbulut, s.361; Dülger, s.460; Korkmaz, s.54.

Ancak Siber Suç Sözleşmesinin 6. maddesinde taraf devletler için öngörülen suç haline getirme yükümlüğünün kapsamını aşan TCK'nın 245/A maddesi, kanunilik ilkesiyle ve hükmün konuluş amacıyla çelişen bir uygulamanın gelişmemesi için dar ve dikkatli yorumlanmalıdır. Ulaştığımız bu sonuç iki hususu kapsamaktadır. İlki TCK'nın 245/A maddesinde kullanılan "..*münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda*.." ifadesi ile ilgilidir. Söz konusu ifadenin failin taşıması gereken saike ilişkin olduğu kabul edilmelidir. Daha açık bir anlatım ile bu ifadeden yola çıkarak failin hareketinin suç teşkil etmesi için TCK'nın Bilişim Alanında İşlenen Suçlar Bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen başka bir suçun işlenmesinde faydalanmak veya faydalanılması amacıyla tipe uygun eylemi gerçekleştirmesinin aranması gerektiği sonucuna varılmalıdır. Hükümde belirtilen ifadenin sadece suçun maddi konusunu tanımlamak için kullanıldığı ve suçun failin saikine bakılmaksızın kasten işlenebileceği kabul edilirse sızma testlerini gerçekleştirmek üzere araç teminine yönelik pek çok davranışın cezalandırılması gerekecektir. Bu sonuç, kusur prensibi ve Anayasanın 17. maddesinde yer alan kişinin maddi ve manevi varlığını geliştirme hakkı ile çeliştiği gibi Siber Suç Sözleşmesinin 6. maddesine açıkça aykırı olacaktır.

İkinci husus "*bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar"* ifadesi ile bağlantılıdır. Belirtilen ifadenin kapsamı dar bir yorum ile tespit edilmeli, bilişim sistemlerinin araç olarak kullanılmasının sadece ilgili suçun nitelikli hali olduğu suçlar ile sınırlı olarak anlamlandırılmalıdır. Aksi halde tüm suçlar bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebileceğinden kanun koyucu tarafından yapılmaya çalışılan sınırlama anlamsız hale gelecektir. Düzenleme kanunilik ilkesinin belirlilik esası ile çelişecektir.

Hükmün geniş yorumlanması ihtimalini bertaraf etmek için olması gereken hukuk açısından ise önerimiz, TCK'nın 245/A maddesinin söz konusu hükümde yer alan "..*bilişim alanında işlenen suçlar bölümünde ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması ya da oluşturulması durumunda*" ifadesi kaldırılarak "*…TCK'nın bilişim alanında işlenen suçlar bölümünde düzenlenen suçlarının işlenmesi için hazırlık yapılması amacıyla*" ifadesi kullanılmak suretiyle yeniden formüle edilmesidir.

Son olarak bir düzenleme ihtiyacına işaret etmek istiyoruz. Kanımızca inceleme konumuzu oluşturan suç bakımından kanun koyucunun etkin pişmanlık hükmü oluşturması yararlı olabilir. Bu bağlamda suça konu cihaz, program, şifre veya sair güvenlik kodunu kabul eden, satın alan, bulunduran

veya depolayan failin soruşturma başlanmadan suçun maddi konusunu pişmanlık göstererek yetkili mercilere teslim etmesinin şahsi cezasızlık nedeni olarak düzenlenmesinin TCK'nın 245/A maddesinin amacıyla bağdaşır yararlı sonuçlar vereceği kanaatindeyiz.

KAYNAKÇA

- Ahmet Gül, *Doğrudan - Dolaylı Bilişim Suçları*, 2. Baskı, Ankara 2018,
- Alisherov A Farkhod ve Sattarova Y Feruza, "Methodology for Penetration Testing", *International Journal of Grid and Distributed Computing,* Vol.2, No.2, June 2009, ss.43-50,
- Andrew Tang, "A Guide to Penetration Testing", *Network Security,* Vol. 2014, Iss. 8, August 2014, ss.8-11,
- Bahri Öztürk ve Mustafa Ruhan Erdem, *Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri*,19. Baskı, Ankara 2019,
- Berrin Akbulut, *Bilişim Alanında Suçlar*, 2. Baskı, Ankara 2017,
- Cahit Aliusta ve Recep Benzer, "Avrupa Siber Suç Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, C.4, S.2, 2018, ss. 35-42,
- Council of Europe, *Explanatory Report to the Convention on Cybercrime ETS 185*, https://rm.coe.int/16800cce5b, (11.12.2019),
- Gunther Arzt, Ulrich Weber, Bernd Heinrich ve Eric Hilgendorf, *Strafrecht Besonderer Teil*, Bielefeld 2009,
- İbrahim Korkmaz, "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu", *Terazi Hukuk Dergisi*, C.13, S.142, Haziran 2018, ss.45-55.
- İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler*, 14. Baskı, Ankara 2018,
- Jörg Eisele, *Strafrecht - Besonderer Teil I,* Stuttgart 2012,
- Kayıhan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, C.59, S.1-2, 2001, ss.3-10,
- Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, 6. Baskı, Ankara 2019,
- Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, 12. Baskı, Ankara 2019,
- Merve Erdem ve Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C.68, S. 1, 2019, ss.127-212,

- Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Özel Sayı Prof. Dr. Nur Centel'e Armağan*, C.19, S.2, 2013, ss.1229-1269,
- Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 7. Baskı, Ankara 2018,
- Mustafa Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, İstanbul 2018,
- Ömer Çıtak, *Ethical Offenssive- Defensive Hacking*, 11. Baskı, İstanbul 2019,
- Önder Tozman, *Suça Teşebbüs*, Ankara 2015,
- Timur Demirbaş, *Ceza Hukuku Genel Hükümler*, 14. Baskı, Ankara 2019,
- TÜBA, *Türkçe Bilim Terimleri Sözlüğü*, http://www.tubaterim.gov.tr/, (11.12.2019),
- Türk Dil Kurumu, *Güncel Türk Sözlük*, https://sozluk.gov.tr/, (11.12.2019),
- Türkan Yalçın Sancar, *Çok Failli Suçlar*, Ankara 1998,
- Türkiye Bankalar Birliği, *Bankacılıkta Dolandırıcılık Eylemleri, Tespit ve Önleme Yöntemleri*, https://www.tbb.org.tr/gec/KTPV14.pdf, (11.12.2019),
- Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, 14. Baskı, Ankara 2019,
- Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, 10. Baskı, Ankara 2019.