

7545 SAYILI SİBER GÜVENLİK KANUNU'NDA DÜZENLENEN SUÇLAR

Offences Regulated in Cyber Security Law No. 7545

Cem ŞENOL*

Özet

Bu çalışma, 7545 sayılı Siber Güvenlik Kanunu'nun 16. maddesiyle Türk hukukunda ilk kez düzenlenen dokuz farklı suç tipini el almaktadır. Siber güvenlik, teknolojinin gelişmesi ile birlikte gündelik hayatın en önemli konularından biri haline gelmiş; Kanun tarafından da milli güvenliğin ayrılmaz bir parçası olarak tanımlanmıştır. Konu Türk hukukunda ilk kez, 12 Mart 2025 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren 7545 sayılı Kanun ile yasal düzenlemeye kavuşmuştur. Bu Kanun'un 16. maddesinde dokuz ayrı suç tipine yer verilerek siber güvenlik alanında işlenebilecek suçlar düzenlenmiş, böylece Türk hukukunda bundan sonra önemli bir uygulama alanı bulacak yeni suç tipleri yaratılmıştır. Çalışmada bu suç tipleri suç incelemesi yöntemi ile incelenerek hem konuya ilişkin literatürün oluşmasına katkı sağlanması hem de söz konusu suç tiplerine ilişkin sorunlu noktaların ve eksikliklerin tespit edilmesi amaçlanmıştır.

Anahtar Kelimeler: Siber, saldırı, veri, siber uzay, yazılım

Abstract

This study examines nine different types of offences regulated for the first time in Turkish law by Article 16 of the Cyber Security Law No. 7545. The development of technology has resulted in cyber security becoming a significant aspect of day-to-day life. Indeed, it has been enshrined in legislation as an integral part of national security. However, the issue has now been regulated for the first time in Turkish law with the Law No. 7545, which came into force after being published in the Official Gazette dated 12 March 2025. Article 16 of the aforementioned regulation stipulates the various offences that may be perpetrated within the sphere of cyber security. The provision incorporates nine different types of offence, thereby establishing new areas of application for Turkish law from here further on. The aim of this study is to contribute to the literature on the subject and to identify the problems and shortcomings associated with these types of crime by examining them using the method of crime analysis.

Key Words: Cyber, cyber attack, data, cyberspace, software

➤ Bu makale Etik Kurul iznine tabi değildir/This article is not subject to Ethics Committee permission.

➤ Makale Geliş Tarihi/Article Received Date: 12.05.2025

➤ Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 22.07.2025

* Doç. Dr., Atatürk Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, cemsenol@atauni.edu.tr, <https://orcid.org/0000-0003-2970-2279>

GİRİŞ

19/3/2025 tarihli ve 32846 sayılı Resmî Gazete’de yayımlanan 7545 sayılı Siber Güvenlik Kanunu (SiGüK) ile siber güvenlik Türkiye hukukunda ilk kez bir kanun ile düzenlenmiştir. Böylece söz konusu Kanun’un kapsam başlıklı 2. maddesi gereğince, güvenlik alanında faaliyet gösteren Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, Milli İstihbarat Teşkilatı ve Türk Silahlı Kuvvetlerinin tabi oldukları kanunlar uyarınca yürüttükleri hariç olmak üzere (SiGüK m.2,f.2)¹, siber uzayda varlık gösteren, faaliyet yürüten, hizmet sunan kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşların siber uzaydaki faaliyetleri yasal düzenlemeye kavuşmuştur.

Böylesi bir yasal düzenleme yapılmasının amacı, Kanun’un “amaç” başlıklı 1. maddesinde, Türkiye Cumhuriyeti’nin siber uzaydaki milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel tehditlerin tespit ve bertaraf edilmesi, siber olayların muhtemel etkilerini azaltmaya yönelik esasların belirlenmesi, kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşların siber saldırılara karşı korunmasına yönelik gerekli düzenlemelerin yapılması, ülkenin siber güvenliğini güçlendirmek için strateji ve politikaların belirlenmesi ile Siber Güvenlik Kurulunun kurulmasına ilişkin esasların düzenlenmesi olarak gösterilmiştir. Bu düzenleme kapsamında da Kanun’un “cezaî hükümler ve idari para cezaları” başlıklı 16. maddesinde, 10. ve 11. fıkralarda düzenlenen iki ayrı kabahatin yanı sıra, farklı fıkralarda yapılan düzenlemeler ile Türk ceza hukuku müktesebatına yeni suç tipleri dahil edilmiştir.

SiGüK m.16 incelendiğinde, Kanun’un 1, 2., 3., 4., 5., 6., 8. ve 9. fıkralarında dokuz farklı suç tipine yer verildiği görülmektedir. Bunlar, 16. maddenin 1. fıkrasında düzenlenen Kanunla yetkilendirilen mercilerin ve denetim görevlilerinin görev ve yetkileri kapsamında istedikleri bilgi, belge, yazılım, veri ve donanımı vermeme veya bunların alınmasına engel olma, 2. fıkrasında düzenlenen, Kanunun alınması gerekli onay, yetki veya izinleri almaksızın faaliyet yürütme, 3. fıkrasında düzenlenen sır saklama yükümlülüğünün ihlali, 4. fıkrasında düzenlenen sızıntı sonucu oluşan verileri erişime açma, paylaşma veya satışa çıkarma, 5. fıkrasında düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma veya yayma, 6. fıkrasının birinci cümlesinde düzenlenen siber saldırı, 6. fıkranın ikinci cümlesinde düzenlenen siber saldırı sonucunda elde ettiği veriyi yayma,

¹ Siber Güvenlik Kanunu 2.madde 2. fıkra: “4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu ve 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu uyarınca yürütülen istihbari faaliyetler ile 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ile 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu uyarınca yürütülen faaliyetler bu Kanun kapsamı dışındadır”.

8. fıkrasında düzenlenen yasak hükümlere aykırı davranma ve 9. fıkrasında düzenlenen görevi ve yetkiyi kötüye kullanma suçlarıdır.

I. KORUNAN HUKUKİ DEĞER

Korunan hukuki değer, toplumsal düzenin barış içerisinde sürdürülmesi için korunması gereken soyut manevi değerler olarak kabul edilmektedir². SiGüK'nun amacı Kanun'un 1. maddesinde, Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren bütün unsurlara karşı içten ve dıştan yöneltilen mevcut ve muhtemel tehditlerin tespit ve bertaraf edilmesi olarak belirlenmiştir. Yine temel ilkeleri düzenleyen m.4, f.1'de de siber güvenliğin, milli güvenliğin ayrılmaz bir parçası olduğu ifade edilmiştir. Dolayısıyla SiGüK m.16'da düzenlenen suçlar ile korunan öncelikli hukuki değer Kanun'un milli güvenliğin bir parçası olarak kabul ettiği ülkenin siber uzaydaki güvenliği ve toplumun buna duyduğu güven duygusu olduğunu söylemek yanlış olmaz.

Bunun yanı sıra Kanun'da düzenlenen dokuz ayrı suç tipi değerlendirildiğinde, suç tiplerinin üç kategoriye bölünmesinin mümkün olduğu söylenebilir. Buna göre suç tiplerinden bir kısmının, siber güvenlik alandaki faaliyetlerin devlet kontrolünde disiplinli bir biçimde yürütülmesini sağlamaya, bir kısmının siber güvenlik alanının ve bu alanda yer alan verilerin korunmasına bir kısmının da siber güvenlik alanında çalışan kişilerin görevin gereklerine aykırı hareketlerini cezalandırılmaya yönelik olarak ihdas edildiğini söylemek hatalı olmaz. Söz konusu suç tipleri ile ihdas edilmelerindeki bu amaçlara göre farklı hukuki değerlerin de korunması amaçlanmıştır.

SiGüK m.16, f.1'de düzenlenen istenen bilgi, belge, yazılım, veri ve donanımı vermeme veya bunların alınmasına engel olma suçu ile 2. fıkra da düzenlenen kanunen alınması gerekli onay, yetki veya izinleri almaksızın faaliyette bulunma suçu siber güvenlik alandaki faaliyetlerin devlet kontrolünde disiplinli bir biçimde yürütülmesini sağlamaya matuftur. Bu sebeple söz konusu suçlar ile korunan hukuki değer, kamunun ve devletin, kamusal nitelikteki siber güvenlik alanındaki faaliyetin disiplinli, hukuka uygun ve düzgün işlemesine ilişkin menfaati ve buna duyulan güven duygusudur.

Buna karşın SiGüK m.16, f.4'te düzenlenen sızıntı sonucu oluşan verileri erişime açma, paylaşma ve satışa çıkarma suçu, aynı maddenin 6. fıkrasının birinci cümlesinde düzenlenen siber saldırı suçu ile ikinci cümlesinde düzenlenen siber saldırı sonucunda elde edilen veriyi yayma suçları siber güvenlik alanının ve bu alanda yer alan verilerin korunmasına matuf suçlar olduğu için, bu suçlar ile ko-

² Mehmet Emin Artuk, Ahmet Gökcen, M. Emin Alşahin, Kerim Çakır, *Ceza Hukuku Genel Hükümler*, (16. Baskı, Adalet Yayınevi, Ankara 2022) 397; Berrin Akbulut, *Ceza Hukuku Genel Hükümler*, (9. Baskı, Adalet Yayınevi, Ankara 2022), 35.



runan diğer hukuki değerlerin, kişilerin bilişim sistemlerinin güvenliği, verilerinin ve özel hayatının gizliliği ile malvarlığı değerleri olduğunu söylemek gerekir.

SiGüK m.16, f.3'te düzenlenen sır saklama yükümlülüğünün ihlali, f.8'de düzenlenen yasak hükümlere aykırı davranma, f.9'da düzenlenen görevi ve yetkiyi kötüye kullanma suçları ise bu alanda çalışan görevlilerin görevin gereklerine aykırı hareketlerini cezalandırmaya matuftur. Bu sebeple mezkûr suçlar ile korunan bir diğer hukuki değer, kamunun, kamu idarelerinin ve kamusal faaliyetin hukukten belirlenen sınırlar içerisinde disiplinli ve dürüst bir biçimde işlediği, kamu görevlilerinin görevin gereklerine uygun hareket ettiği konusunda duyduğu güven duygusudur.

SiGüK m.16, f.5'te düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma ve yayma suçu ile korunmak istenen hukuki değer ise kamu barışıdır.

II. FAİL

Kanun koyucu SiGüK m.16'da düzenlenen suçlardan 3. fıkra da düzenlenen sır saklama yükümlülüğünün ihlali, 8. fıkra da düzenlenen yasak hükümlere aykırı davranma suçu ve 9. fıkra da düzenlenen görevi ve yetkiyi kötüye kullanma suçları dışındaki suçlarda, bir kişinin suçun faili olabilmesi için herhangi bir sıfat veya özelliğe sahip olmasını aramamıştır. Bu sebeple söz konusu suçlar, herkes tarafından işlenebilen suçlardandır³.

Buna karşılık bir kişinin m.16, f.3'de düzenlenen sır saklama yükümlülüğünün ihlali suçunun faili olabilmesi için, Kanun'un 13. maddesi gereğince Siber Güvenlik Başkanlığı (SGB) tarafından yürütülen görev ve faaliyetler kapsamında kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgiler, kişisel veriler, ticari sırlar ve bunlara ait belgeleri edinmiş olması nedeniyle bu bilgi ve belgeleri ilgili mevzuat gereği yetkili kılınan mercilerden başkasına açıklamama, gerçek ve tüzel kişilerin menfaatine kullanmama yükümlülüğü altında olması gerekir. Dolayısıyla bu suç, herkes tarafından işlenemeyecek, sadece belirtilen hukuki durumda bulunan belli kişiler tarafından yükümlülüğün ihlaliyle işlenebilecek bir yükümlülük suçudur⁴.

SiGüK m.16, f.8'de düzenlenen yasak hükümlere aykırı davranma suçunun faili, SiGüK ile kurulan SGB'de kadrolu veya sözleşmeli statüde görev yapmış olmasına karşın Kanun'un 12. maddesinde sayılan yasaklanmış fiilleri icra eden kişilerdir. SGB, kanunla kurulmuş bir kamu kurumudur. Dolayısıyla bu kurumda kadrolu veya sözleşmeli statüsünde çalışan kişiler, Türk Ceza Kanunu⁵ m.6, f.1

³ İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler*, (18. Baskı, Seçkin Yayıncılık, Ankara 2022) 212; Hakan Karakehya, *Ceza Hukuku Genel Hükümler*, (Adalet Yayınevi, Ankara 2022) 66.

⁴ Özgenç (n3) 212.

⁵ 12.10.2004 tarihli ve 25611 sayılı Resmî Gazete'de yayınlanmıştır.

gereğince ceza kanunlarının uygulanması açısından kamu görevlisi statüsündedir⁶. Kanun'un 16. maddesinin 9. fıkrasında düzenlenen görevi kötüye kullanma ile görevin gereklerine aykırı hareket etmek suretiyle veri ihlaline sebebiyet verme suçlarının faili de sadece SiGüK ile kendilerine verilen görev ve yetkiyi kötüye kullananlar ile görevin gereklerine aykırı hareket etmek suretiyle veri ihlali yaşanmasına sebebiyet veren yetkili kişiler olabilir. Bu kişiler, SGB çalışanları veya Başkanlığın Kanun'un kendine tanıdığı yetkiye dayanarak faaliyetlerine izin veya onay verdiği kurumların personeli olabilir. Bu sebeple söz konusu suçlar, herkes tarafından işlenemeyecek faili bakımından özgü suç niteliğinde suçlardır⁷.

TCK m.16'da düzenlenen suçlar arasında ne birleşme ne de karşılaşma şeklinde çok failli suçlara yer verilmediği görülmektedir. Bu sebeple maddede düzenlenen suçların tamamı, failin sayısı bakımından tek failli suçtur.

III. MAĞDUR

Suçun mağduru, suçla korunan hukuki değer sahibi olan kişi veya kişilerdir. Suçla korunan hukuki değer bir kişi veya belli kişilere ait olduğu suçlarda mağdur, bu kişi veya kişilerdir. Buna karşın suçla korunan hukuki değer tüm topluma ait olduğu suçlarda ise mağdur, tüm toplumdur⁸.

SiGüK ile düzenlenen suçlara baktığımızda, bir kısmının siber uzay olarak tabir edilen yerdeki genel işleyişin ve faaliyetlerin sorunsuz ve kesintisiz olarak yürütülmesine yönelik olduğu, 5. fıkrasında düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma ve yayma suçunun ise kamu barışını korumak amacıyla düzenlendiği, suçların bir kısmı ile korunmak istenen hukuki değerlerin ise bilişim sistemlerinin ve kişilerin veya kurumların veri güvenliğini sağlamak olduğu görülmektedir. Bu sebeple Kanun'da düzenlenen suçların mağduru bakımından kişilerin ve tüm toplumun mağdur olduğu suçlar olarak ikiye ayrıldığını söylemek yanlış olmaz.

Kanun'da düzenlenen suçlardan 5. fıkrada düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma ve yayma suçu ile korunmak istenen hukuki değer kamu barışı olduğu için, bu suçun mağduru tüm toplumdur⁹. Yine f.3'te düzenlenen sır saklama yükümlülüğünün ihlali, f.8'de düzenlenen yasak hükümlere aykırı davranma, f.9'da düzenlenen görevi ve yetkiyi kötüye kullanma suçları ile korunan hukuki değer, kamunun, kamu idarelerinin ve kamusal faaliyetin hukuken belirle-

⁶ Kamu görevlisi kavramı hakkında bakınız: Mahmut Kaplan, "Türk Ceza Hukukunda Kamu Görevlisi Kavramı", (Aralık 2015) 5(2), *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, 61 vd.

⁷ Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, *Ceza Hukuku Genel Hükümler*, (15. Baskı, Seçkin Yayıncılık, Ankara 2024) 219; Hakan Hakeri, *Ceza Hukuku Genel Hükümler*, (23. Baskı, Adalet Yayınevi, Ankara 2020) 142.

⁸ Artuk, Gökçen, Alşahin, Çakır (n2) 392; Karakehya (n3) 69.

⁹ Cem Şenol, "Halkı Yanıltıcı Bilgiyi Alenen Yayma Suçu", (Aralık 2022), 17(20), *Ceza Hukuku Dergisi*, 337.



nen sınırlar içerisinde disiplinli ve dürüst bir biçimde işlediği, kamu görevlilerinin görevin gereklerine uygun hareket ettiği konusunda duyduğu güven duygusudur. Bu sebeple anılan suçların mağduru, bütün toplumdur¹⁰. SiGüK m.16, f.1'de düzenlenen kanunla yetkilendirilen mercilerin ve denetim görevlilerinin görev ve yetkileri kapsamında istedikleri bilgi, belge, yazılım, veri ve donanımı vermeme veya bunların alınmasına engel olma suçu ile SiGüK m.16, f.2'de düzenlenen kanunun alınması gerekli onay, yetki veya izinleri almaksızın faaliyet yürütme suçu ile korunan hukuki değer, kamunun ve devletin kamusal nitelikteki siber güvenlik faaliyetinin disiplinli, hukuka uygun ve düzgün işlemesine ilişkin menfaati ve buna duyduğu güven duygusudur. Bu sebeple mezkûr suçların mağduru, bütün toplumdur.

Buna karşın SiGüK m.16, f.4'te düzenlenen sızıntı sonucu oluşan verileri erişime açma, paylaşma ve satışa çıkarma suçu, aynı maddenin 6. fıkrasının birinci cümlesinde düzenlenen siber saldırı suçu ile ikinci cümlesinde düzenlenen siber saldırı sonucunda elde edilen veriyi yayma suçları ile korunan hukuki değer, kişilerin bilişim sistemlerinin güvenliği, verilerinin ve özel hayatının gizliliği ile malvarlığı değerleridir¹¹. Bu sebeple bu suçlarda bilişim sistemleri siber saldırıya maruz kalan gerçek veya tüzel kişiler ile gizliliği ihlal edilerek verileri elde edilen, yayılan, satılan, erişime açılan, paylaşılan veya satışa çıkarılan kişiler suçun mağduru olur¹². Ancak bu suçlardan siber saldırı suçu ile korunan asıl hukuki değer kamunun siber uzaydaki faaliyetlerin güven içerisinde yürütülmesine duyduğu güven duygusu olduğunun kabul edilmesi durumunda bu suçun mağdurunun kamu, suçtan zarar göreninin ise siber saldırıya uğrayan gerçek ve tüzel kişiler olduğunu söylemek mümkün gözükmemektedir.

IV. FİİL

SiGüK'nın 16. maddesinde dokuz ayrı suç tipi, genellikle birden farklı seçimlik hareketin icrasıyla işlenebilecek şekilde düzenlenmiştir. Bu sebeple çalışmanın bu kısmında söz konusu suçların fiil unsuru ayrı ayrı ele alınacaktır.

A. İSTENEN BİLGİ, BELGE, YAZILIM, VERİ VE DONANIMI VERMEME VEYA BUNLARIN ALINMASINA ENGEL OLMA SUÇU (SiGüK m.16, f.1)

SiGüK m.16, f.1'de, kamu kurum ve kuruluşları hariç olmak üzere söz konusu Kanun ile yetkilendirilen mercilerin ve denetim görevlilerinin görev ve yetkileri kapsamında istedikleri bilgi, belge, yazılım, veri ve donanımın verilmemesi veya bunların alınmasına engel olunması suç olarak düzenlenmiştir.

¹⁰ Muharrem Özen, Köksal Atacan, "Göreve İlişkin Sırrın Açıklanması Suçu", (2020), 69(1), *Ankara Üni. Hukuk Fak. Dergisi*, 197; Handan Yokuş Sevük, "Görevi Kötüye Kullanma Suçu (TCK m.257)", (2018), 23(39), *DÜHFD*, 262, 267; Güneş Okuyucu Ergün, "Görevi Kötüye Kullanma Suçu", (2009), (82), *TBB Dergisi*, 2, 3.

¹¹ Bilişim suçları ile korunan hukuki değerler konusunda bakınız: Berrin Akbulut, *Bilişim Suçları*, (2. Baskı, Adalet Yayınevi, Ankara 2017) 117.

¹² Karşılaştırınız: Akbulut (n11) 121.

SGB, Kanun'un 8. maddesi gereğince, Kanun'da belirtilen görevleri ile ilgili olarak gerekli gördüğü hallerde Kanun'un kapsamına giren her türlü fiil ve işlemi denetleyebilir, bu amaçla mahallinde inceleme yapabilir veya yaptırabilir. Denetim, bu Kanun kapsamındaki kurum, kuruluş ve ilgili diğer gerçek ve tüzel kişilerin bu Kanun hükümleriyle ilgili faaliyet ve işlemlerini kapsar. Denetime, Başkanlık personeli, yetkilendirilmiş ve belgelendirilmiş bağımsız denetçiler ve bağımsız denetim kuruluşları yetkilidir. Bu yetki, Başkan tarafından görevlendirilenler tarafından kullanılır. Kamu kurum ve kuruluşları ile kritik altyapılarda denetimler, Başkanlık personeline veya refakatinde yapılır. Bu sebeple mülki amirler, kolluk kuvvetleri ve diğer kamu kurumlarının amir ve memurları inceleme veya denetimle görevlendirilenlere her türlü kolaylığı göstermek ve yardımda bulunmakla yükümlüdürler. Denetimle görevlendirilenler; yapılan denetimler sırasında yürüttükleri denetim faaliyetleriyle sınırlı olarak elektronik ortamdaki verinin, belgelerin, elektronik altyapının, cihaz, sistem, yazılım ve donanımlarının incelenmesi, bunlardan kopya, dijital suret veya örnek alınması, konuyla ilgili yazılı veya sözlü açıklama istenmesi, gerekli tutanakların düzenlenmesi, tesislerin ve işletiminin incelenmesi konularında yetkilidir. Denetime tabi tutulanlar, ilgili cihaz, sistem, yazılım ve donanımları verilen sürelerde denetlemeye açık tutmak, denetim için gerekli altyapıyı temin etmek ve çalışır vaziyette tutmak için gerekli önlemleri almak zorundadır (SiGüK m.8, f.1, 3, 4). Yine SiGüK gereğince SGB ve onun SiGüK m.6, f.1-ğ'nin tanıdığı yetkiyle kendisini yetkilendirdiği bağımsız denetçiler ve denetim kuruluşları da Kanun'un kapsamındakilerden, yürüttüğü faaliyetlerle sınırlı olmak üzere bilgi, belge, veri ve kayıtları alabilir ve bunların değerlendirmesini yapabilir; bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir. Bu kapsamda elde edilen bilgi, belge, veri ve kayıtlar, en fazla iki yıl süreyle çalışmaya konu edilir ve çalışma süresi sonrasında imha edilir. Bu kapsamda kendisinden herhangi bir talepte bulunulanlar, kendi mevzuatındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınmaz. Başkanlık, bilişim sistemlerindeki log kayıtlarını bünyesinde toplayabilir, saklayabilir, değerlendirebilir. Bunlar hakkında rapor hazırlayarak ilgili kurum ve kuruluşlar ile paylaşabilir (SiGüK m.6, f.1-ç, d).

SiGüK m.16, f.1'de düzenlenen istenen bilgi, belge, yazılım, veri ve donanım vermeme veya bunların alınmasına engel olma suçu, SGB'ye yukarıda izah edilen denetim yetkisi kapsamında toplanma yetkisi verilmiş suçun konusunu oluşturan bilgi, belge, yazılım, veri ve donanımın talep üzerine verilmemesi veya alınmasına engel olma şeklinde iki ayrı seçimlik hareketle işlenebilen seçimlik hareketli bir suçtur. Suç seçimlik hareketli suç olduğundan, işlenmesi için failin kanuni tanımda sayılan üç ayrı seçimlik hareketten birisini icra etmesi yeterli-



dir. Failin seçimlik hareketlerden birden fazlasını icra etmesi durumunda yine tek suç oluşur. Ancak bu durum, temel cezanın belirlenmesinde dikkate alınır¹³.

Suçun seçimlik hareketlerinden olan istenen bilgi, belge, yazılım, veri ve donanımı vermeme, söz konusu unsurların denetim görevlilerine teslim edilmesine yönelik verme emrinin ihlali ile işleneceğinden gerçek ihmali bir suçtur¹⁴. Suçun bu seçimlik hareketi bir yükümlülüğün yerine getirilmemesiyle işlenen bir gerçek ihmali suç olduğu için, oluşması, somut olayda failin suçun konusunu oluşturan hususları teslim etme yükümlülüğünün doğmasına bağlıdır.¹⁵ Bu sebeple teslim etmesi istenen kişi ve kuruluşların, teslimi istenen şeylerin neler olduğu, hangi süre içerisinde, kime, nerede ve nasıl teslim edilmesinin istendiği hususlarında uygun araçlarla açıkça bilgilendirilmesi gerekir. Bu çerçevede suçun bu seçimlik hareketi, denetim yetkisine sahip olan kurumların, bu yetki çerçevesinde kamu kurumu niteliğindeki meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşlardan kendilerine ait bilgi, belge, yazılım, veri ve donanımın kendisine teslim edilmesini talep etmesi, ancak söz konusu kişi ve kuruluşların bu konudaki talebi yerine getirmeyerek istenen hususları teslim etmemesiyle oluşur. Suç, teslimi, istenen şeylerin teslimi için tanınan sürenin sona ermesi ile birlikte tamamlanır¹⁶.

Suçun ikinci seçimlik hareketi olan istenilen bilgi, belge, yazılım, veri ve donanımın alınmasına engel olma ise kamu kurum ve kuruluşları dışında kalan kişi ve birimlerin, SiGüK m.8, f.4 gereğince denetimle görevlendirilenler tarafından yürütülen denetim faaliyetleri sırasında elektronik ortamdaki verinin, belgelerin, elektronik altyapının, cihaz, sistem, yazılım ve donanımlarını incelemesi, bunlardan kopya, dijital suret veya örnek alması, konuyla ilgili yazılı veya sözlü açıklama istemesi, gerekli tutanakları düzenlemesi, tesisleri ve işletimini incelemesi yetkisinin fiilen kullanılması sırasında ortaya çıkabilir. Bu kapsamda denetimi yapanların bu sırada söz konusu belgelerden, elektronik altyapı, cihaz, sistem, yazılım ve donanımlardan kopya, dijital suret veya örnek almaya çalışmasına karşı engellenmesi durumunda, suçun bu seçimlik hareketi oluşur. Bu bakımdan suçun bu seçimlik hareketi, ilk seçimlik hareketinin aksine, failin engelleme şeklinde aktif bir karşı koyma davranışıyla işlenebilecek icrai bir suçtur.

¹³ Mahmut Koca, İlhan Üzülmaz, *Türk Ceza Hukuku Genel Hükümler*, (15. Baskı, Seçkin Yayıncılık, Ankara 2022) 124; Artuk, Gökcen, Alşahin, Çakır (n2) 336.

¹⁴ Özgenç (n3) 391; Koca, Üzülmaz (n13) 394; Hakeri (n7) 170.

¹⁵ Koca, Üzülmaz (n13) 394; Özbek, Doğan, Bacaksız (n7) 532; Hakeri (n7) 172.

¹⁶ Artuk, Gökcen, Alşahin, Çakır (n2) 339; Hakeri (n7) 510.



B. KANUNEN ALINMASI GEREKLİ ONAY, YETKİ VEYA İZİNLERİ ALMAKSIZIN FAALİYET YÜRÜTME SUÇU (SiGüK m.16, f.2)

SiGüK m.16, f.2’de düzenlenen kanunen alınması gerekli onay, yetki veya izinleri almaksızın faaliyet yürütme suçu, Siber Güvenlik Kanunu’nun uygulama alanına giren bir konuda faaliyet gösteren kişi veya kurumların, söz konusu faaliyetin yürütülmesinin onay, yetki veya izne tabi olmasına rağmen, bu onay, yetki veya izni almaksızın faaliyet göstermesini suç olarak düzenlenmektedir. Bu sebeple suçun fiil unsurunun oluşması için, failin Kanun’a göre faaliyet göstermek için onay, yetki veya izin almasının gerekli olması ve buna rağmen söz konusu izinleri almaksızın siber güvenlik alanında hukuka aykırı olarak fiilen faaliyet göstermesi gerekir. Bu bakımdan suç, Kanun’un emrettiği onay, yetki, izin almadan faaliyet yürütme yasağının ihlali suretiyle işlenebilecek icrai bir suçtur¹⁷.

Suçun oluşması için varlığı gereken birinci koşul, ilgili kişi veya kurumun siber güvenlik alanında faaliyet göstermesi için Kanun gereği bir onay, yetki veya izin almasının gerekmesidir. Kanun’un incelenmesinden buna ilişkin bir hükme, Kanun’un geçici madde 1, f.4’te siber güvenlik alanında faaliyet icra eden dernek, derneklerden oluşan federasyonlar, vakıflar ile ticaret şirketleri açısından yer verildiği görülmektedir. Buna göre adı geçen özel hukuk tüzel kişileri, aynı maddenin altıncı fıkrasında belirtilen Kanun’un uygulanmasına ilişkin düzenlemelerin yürürlüğe girmesinden itibaren bir yıl içerisinde Başkanlığın belirlediği ilke ve esaslar çerçevesinde sertifikasyon, yetkilendirme ve belgelendirme işlemlerini tamamlamakla yükümlüdürler. Bu yükümlülüğün yerine getirilmemesi halinde siber güvenlik alanında faaliyette bulunamazlar. Dolayısıyla bu düzenlemede belirtilen onay, yetkilendirme ve izinlerin SiGüK m.16, f.2’de düzenlenen suçun konu unsurunu oluşturacağı açıktır. Yine Kanun m.7, f.1-ç gereğince ilk kez siber güvenlik alanında faaliyet gösterecek sertifikasyon, yetkilendirme ve belgelendirmeye tâbi siber güvenlik şirketlerinin faaliyete başlamadan önce mevcut düzenlemeler çerçevesinde Başkanlıktan almaları gereken onay da bu suçun konusunu oluşturur. Buna karşın SiGüK m.5 f.1-e’de SGB’nin görevleri arasında siber güvenlik alanında faaliyet gösterenlerin uyması gereken usul ve esasları düzenlemek sayılmış olsa da Başkanlığın söz konusu fıkranın verdiği yetkiye dayanarak çıkaracağı genel düzenleyici işlemlerde yer alan hükümlerin bu suçun konusunu oluşturması, TCK m.2’de düzenlenen suçların kanuniliği ilkesi nedeniyle mümkün değildir¹⁸. Yine SiGüK m.12, f.1’de SGB bünyesinden ayrılmış kişilere yönelik düzenlenen muvafakat ve f.2’de düzenlenen yetkilendirme koşulları, 12. maddede düzenlenen hususlara aykırı davranmak SiGüK m.16, f.8’de ayrıca suç olarak düzenlediği için, f.2’de düzenlenen suçun konusunu oluşturmaz.

¹⁷ Artuk, Gökçen, Alşahin, Çakır (n2) 337; Akbulut (n2) 349.

¹⁸ Özgenç (n3) 121; Karakehya (n3) 32.



C. SIR SAKLAMAYÜKÜMLÜLÜĞÜNÜN İHLALI SUÇU (SiGüK m.16, f.3)

SiGüK m.16, f.3'te düzenlenen sır saklama yükümlülüğünün ihlali suçunun fiil unsuru, kişinin, suçun konusunu oluşturan SGB tarafından yürütülen görev ve faaliyetler kapsamında edindiği, kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri veya kişisel verileri ya da ticari sırları ve bunlara ait belgeleri, mevzuat gereği yetkili kılınan mercilerden başkasına açıklamasıyla ya da gerçek ve tüzel kişilerin menfaatine kullanmasıyla oluşur. Bu bakımdan suç, failin yürüttüğü görev nedeniyle sır saklama şeklinde kendisine yüklenen bir yükümlülüğün, yani yasak normunun ihlali ile işlendiği için icrai hareketli bir suçtur¹⁹.

Suç, failin saklamakla yükümlü olduğu sır niteliğindeki bilgi veya belgele-ri açıklaması ya da gerçek ve tüzel kişilerin menfaatine kullanması şeklinde iki seçimlik hareketten birinin icrasıyla işlenebilir. Bu yüzden seçimlik hareketli bir suçtur. Seçimlik hareketli suçlarda failin seçimlik hareketlerden birden fazlasını icra etmesi durumunda yine de tek suç oluşacağından, failin başkasına açıklama ve menfaatine kullanma seçimlik hareketlerinden her ikisini de ihlal etmesi durumunda tek suç oluşur, ancak faile alt sınırdan uzaklaşarak ceza verilir²⁰.

İfşa ile aynı anlama gelen açıklanma, gizli, yani başkalarının bilinmeyen bir bilgi veya belgenin gizlilik vasfı ihlal edilerek bilgi sahibi olmayan kişiler tarafından bilinebilir hale getirilmesidir²¹. Açıklanma fiilinin oluştuğundan bahsedilebilmesi için, bilgi veya belgenin, o bilgi veya belge kendisine gizli olan en az bir kişiye aktarılması yeterlidir. Açıklama fiilinin tamamlanması için muhatabın açıklanan bilgi veya belgeyi öğrenmesi gerekmez; fiil, failin bilgi veya belgeyi aktarmasıyla tamamlanmış olur²². Bu sebeple suç ani hareketli bir sırf hareket suçudur. Ayrıca kanuni tanımda ne şekilde işleneceği konusunda herhangi bir sınırlamaya gidilmediği için serbest hareketli olan suç, bilgi veya belgenin yazılı, sözlü, görsel olarak herhangi bir şekilde ifşasıyla işlenebilir²³. Ancak bilginin veya belgenin açıklandığından bahsedilebilmesi için, suçla korunan hukuki değeri ihlal edebilecek en azından bir kısmının içerik olarak başka kişi veya kişilere iletilmesi gerekir. İçeriğini açıklamadan sadece bilgi veya belgenin varlığının bildirilmesi, açıklama fiilini oluşturmaz²⁴. Son olarak kanun koyucu suçun oluşması için bilgi veya belgenin açıklanması durumunda bir zarar veya somut tehlikenin ortaya çıkmasını aramamıştır. Suç, bu sebeple bir soyut tehlike suçudur²⁵.

¹⁹ Artuk, Gökçen, Alşahin, Çakır (n2) 337; Akbulut (n2) 349.

²⁰ Koca, Üzülmüş (n13) 124; Artuk, Gökçen, Alşahin, Çakır (n2) 336.

²¹ Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku*, (20. Baskı, Seçkin Yayıncılık, Ankara 2022) 702; Mahmut Koca, İlhan Üzülmüş, *Türk Ceza Hukuku Özel Hükümler*, (8. Baskı, Adalet Yayınevi, Ankara 2022) 576.

²² Tezcan, Erdem, Önok (n21) 702.

²³ Koca, Üzülmüş (n21) 576.

²⁴ Koca, Üzülmüş (n21) 576.

²⁵ Özgenç (n3) 221.

Sır saklama yükümlülüğünün ihlali suçunun diğer seçimlik hareketini oluşturan sır teşkil eden bilgi veya belgeyi bir gerçek veya tüzel kişinin menfaatine kullanma, sır saklama yükümlülüğü altında olan failin, söz konusu bilgi veya belgeyi bir gerçek veya tüzel kişi lehine çıkar temin etmek için kullanmasını ifade eder. Suçun tipikliğindeki menfaat kavramının, kavram TCK m.79’da düzenlenen göçmen kaçakçılığı suçunda olduğu gibi maddi menfaatler şeklinde sınırlandırılmadığı için, irtikap suçunda olduğu gibi gerçek veya tüzel kişi lehine sağlanan maddi nitelikte olmayanlar da dahil her türlü çıkar ve fayda olarak anlaşılması gerekir²⁶. Bu sebeple örneğin, bir miktar paranın alınması kadar bir tayin işinin yapılması veya çocuğunun aslında kaydolma hakkı olmayan bir okula kaydedilmesi gibi doğrudan ekonomik değeri olmayan menfaatler de suçun konusunu oluşturur. Suçun bu seçimlik hareketinin oluşması için failin sahip olduğu sır teşkil eden bilgi ve belgeyi menfaatine kullanması yeterlidir. Lehine hareket ettiği gerçek veya tüzel kişinin menfaati elde etmiş olması gerekmez. Bu açıdan suç, bu seçimlik hareket bakımından hem sırf hareket suçu hem de oluşması için bir zarar veya tehlikenin ortaya çıkması aranmadığı bir soyut tehlike suçudur.

Suç, kanun koyucu menfaatine kullanma seçimlik hareketinin nasıl işleneceği konusunda herhangi bir sınırlama getirmediği için serbest hareketlidir; menfaat teminine yönelik herhangi bir şekilde işlenebilir. Ayrıca menfaat teminine yönelik hareketin yapılması ile hem tamamlanıp hem de biteceği için de ani hareketlidir²⁷.

D. SIZINTI SONUCU OLUŞAN VERİLERİ ERİŞİME AÇMA, PAYLAŞMA VEYA SATIŞA ÇIKARMA SUÇU (SİGÜK m.16, f.4)

Sızıntı sonucu oluşan verileri erişime açma, paylaşma ve satışa çıkarma suçu, sızıntı sonucu siber uzayda bulunan veriyi, verinin sahibi olan kişilerin veya kurumlardan izin almaksızın ücretli ya da ücretsiz olarak erişime açma, veriyi paylaşma veya satışa çıkarma şeklinde üç farklı hareketle işlenebilen seçimlik hareketli bir suçtur²⁸. Suç seçimlik hareketli bir suç olduğundan, işlenmesi için failin kanuni tanımda sayılan üç ayrı seçimlik hareketten birisini icra etmesi yeterlidir. Failin seçimlik hareketlerden birden fazlasını icra etmesi durumunda yine tek suç oluşur. Ancak bu durum temel cezanın belirlenmesinde dikkate alınır²⁹.

Suçun seçimlik hareketlerinden olan erişime açma, failin suçun konusunu oluşturan veri sızıntısı sonucu siber uzayda bulunan veriye, o veriye ulaşma imkânı olmayan kişilerin erişimlerini mümkün kılmasını ifade eder. Örneğin,

²⁶ Tezcan, Erdem, Önok (n21) 1296; Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, *Ceza Hukuku Özel Hükümler*, (19. Baskı, Seçkin Yayıncılık, Ankara 2024) 1099.

²⁷ Hamide Zafer, *Ceza Hukuku Genel Hükümler*, (8. Bası, Beta Yayın, İstanbul 2021) 262.

²⁸ Bahar Turgut, “Siber Uzayda Yer Alan Kişisel veya Kritik Kamu Hizmeti Kapsamına Giren Kurumsal Verileri Erişime Açma, Paylaşma ve Satışa Çıkarma Suçu”, (Haziran 2025) (16) İnönü Üniversitesi Hukuk Fakültesi Dergisi, s.207 vd.

²⁹ Koca, Üzülmaz (n13) 124; Artuk, Gökçen, Alşahin, Çakır (n2) 336.



failin başka kişilere verinin siber uzayda bulunduğu yere girebilmesi için şifresini vermesi ya da başkalarının erişmesini önlemek için konulan güvenlik duvarı, şifre gibi tedbirleri devre dışı bırakması durumunda bu seçimlik hareket oluşur.

Suçun ikinci seçimlik hareketi olan paylaşma, TCK m.136'da düzenlenen vermek ve yaymak fiillerini birlikte ifade eder. Bu bakımdan bilginin, yazının veya görsel malzemenin başkasına aktarılmasını, elden verilmesini, iletişim araçlarının herhangi biriyle dağıtılmak suretiyle başkalarının öğrenmesinin mümkün kılınmasını ifade eder³⁰. Örneğin, suçun konusunu oluşturan verilerin bir internet sitesine yüklenerek alenileştirilmesi, sosyal medya hesaplarından yayınlanması veya mesajlaşma uygulamalarından başkalarına iletilmesi ya da depolandığı veri depolama cihazlarının elden verilmesi durumunda paylaşma seçimlik hareketi oluşur.

Suçun üçüncü ve son seçimlik hareketi olan satışa çıkarma ise suçun konusunu oluşturan verinin zilyedi olan veya en azından istediğinde erişebilecek durumda olan kişilerin, ücret karşılığı veriyi bir başkasına devretme iradesini gösteren, satmaya yönelik ve satmadan önce gelen tüm hazırlık hareketlerini ifade eder. Müşteri arama, satmayı teklif etme, bir ekonomik menfaat karşılığı anlaşmaya çalışma gibi hareketler, bu seçimlik hareketi oluşturur³¹.

Kanun koyucu suça vücut veren seçimlik hareketlerin ne şekilde işleneceği konusunda bir sınırlamaya gitmemiş, hatta erişime açma ve paylaşma seçimlik hareketlerinin oluşması için bu paylaşımın ücret karşılığı veya ücretsiz yapılması arasında bir fark gözetmemiştir. Bu sebeple suç, serbest hareketli bir suçtur³². Erişime açma ve paylaşma seçimlik hareketlerinin hem ani hem de mütemadi olarak işlenmesi mümkündür. Örneğin paylaşma seçimlik hareketi, verinin mesajlaşma uygulaması ile bir kişiye gönderilmesi durumunda ani hareketli, bir sosyal medya hesabından paylaşılması durumunda mütemadi olarak işlenmiş olur.

Suçun oluşması için erişime açma, paylaşma, satışa çıkarma seçimlik hareketlerinin icrasının nedeniyle verinin ait olduğu kişilerin bir zarar veya tehlikeye uğraması aranmamıştır. Bu sebeple suç, bir soyut tehlike ve sırf hareket suçudur³³.

E. VERİ SIZINTISI HAKKINDA GERÇEĞE AYKIRI İÇERİK OLUŞTURMA VEYA YAYMA SUÇU (SiGüK m.16, f.5)

SiGüK m.16, f.5'te düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma veya yayma suçu, veri sızıntısı gerçekleştiği konusunda gerçeğe aykırı içerik oluşturulması veya gerçeğe aykırı olarak oluşturulan içeriğin yayılması şek-

³⁰ Köksal Bayraktar, *Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar, Özel Ceza Hukuku* (C.III, On İki Levha Yayıncılık, İstanbul 2018) 642.

³¹ Melek Yamaner Özdemir, *Uyuşturucu veya Uyarıcı Madde İmal ve Ticareti Suçu (TCK m.188)*, (Seçkin Yayıncılık, Ankara 2022) 69.

³² Özbek, Doğan, Bacaksız (n7) 235; Zafer (n27) 248.

³³ Özgenç (n3) 221.

linde iki ayrı seçimlik hareketten birisinin icrasıyla işlenebileceğinden seçimlik hareketli bir suçtur. Suç seçimlik hareketli olduğundan, oluşması için failin içerik oluşturma veya oluşturulmuş içeriği yayma şeklindeki iki seçimlik hareketten birisini icra etmesi yeterlidir. Bu bakımdan hem içerik oluşturma hem de yayma fiilinin aynı kişi tarafından işlenmesi gerekmez. Failin her iki seçimlik hareketi de icra etmesi durumunda yine tek suç oluşur³⁴. Ancak bu durumda temel cezanın alt sınırdan uzaklaşılarak belirlenmesi gerekir.

Suçun seçimlik hareketlerinden biri olan veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma, failin ortada bir veri sızıntısı olmadığını bildiği halde, gerçeğe aykırı olarak böylesi bir veri sızıntısı olduğu izlenimi yaratacak yazılı, görsel veya sesli içerikler oluşturma ile işlenir. Örneğin, bir siber saldırı ile ülkede yaşayan kişilerin E Nabız uygulaması üzerinden sağlık bilgilerinin ele geçirildiğini gösteren görsel materyaller hazırlanması veya bu verileri korumakla görevli olduğu iddia edilen bir görevliye ait olduğu iddiasıyla sahte bir ses kaydının hazırlanması durumunda söz konusu seçimlik hareket oluşur. Bu seçimlik hareket, içeriğin oluşturulması ile birlikte hem tamamlanıp hem de biteceği için ani hareketli, suçun kanuni tanımında içeriğin ne şekilde hazırlanacağı konusunda herhangi bir sınırlama getirilmediği için serbest hareketlidir³⁵.

Suçun seçimlik hareketlerinden ikincisi, suçun konusunu oluşturan gerçeğe aykırı olarak oluşturulduğu bilinen içeriğin yayılmasıdır. Bir bilgi veya haber niteliği taşıyan içeriği yaymak, söz konusu içeriği birden çok kimseye duyurması, öğrenmesini sağlaması demektir³⁶. Yayma fiilinin tamamlanması için, yayılan içeriğin diğer kişiler tarafından öğrenilmesi gerekli değildir. Bu nedenle yayma fiili, failin gerçeğe aykırı olarak oluşturulduğunu bildiği içerikleri başkalarının öğrenmesini mümkün kılacak şekilde paylaşması ile işlenir. Suçun fiil unsurunu oluşturan yayma fiilinin gerçekleşmesi için bir veri sızıntısı yaşandığına ilişkin gerçeğe aykırı olduğu bilinen içeriklerin birden çok kişinin vakıf olabileceği şekilde ulaşılabilir kılınması yeterlidir. Yaymanın şekli, suçun oluşması bakımından önem taşımaz. İçerik, yazılı, sesli veya görüntülü olabileceği gibi, yazılı, sözlü, görüntülü ve eylemli olarak da yayılabilir³⁷. Örneğin, böylesi bir içeriğin internet sitesine yüklenmesi, haberleşme uygulamalarında kurulan gruplarda paylaşılması veya bir kişinin sosyal medyada yapılan böylesi bir içeriğe sahip paylaşımını kendi takipçilerinin de görmesi için yeniden iletmesi durumunda yayma fiili gerçekleşmiş olur. Suç bu sebeple serbest hareketlidir³⁸. Yayma seçimlik hareketi, gerçeğe aykırı olarak oluşturulan içeriğin paylaşılmasına yönelik yasak

³⁴ Koca, Üzülmaz (n13) 124; Artuk, Gökçen, Alşahin, Çakır (n2) 336.

³⁵ Özgenç (n3) 184, 191.

³⁶ Bayraktar n(29) 642; Şenol (n9) 334.

³⁷ Şenol (n9) 334.

³⁸ Karakehya (n3) 56.



normun ihlali ile işlenebileceği için icrai hareketli; yayma hareketinin icrası ile hem tamamlanıp hem de sona ereceği için kural olarak ani hareketlidir. Ancak içeriğin, örneğin bir internet sitesinde belli bir süre duracak şekilde yüklenmesi durumunda, içerik sitede durduğu sürece yayma fiilinin icrası devam edeceği için, suç mütemadi şeklide işlenmiş olur³⁹.

Kanun koyucu bu suçun oluşması için her iki seçimlik hareketin icrası sonucunda da herhangi bir zarar veya somut tehlikenin meydana çıkmasını aramamıştır. Bu nedenle suç, bir sırf hareket ve soyut tehlike suçudur⁴⁰.

F. SİBER SALDIRI SUÇU (SiGüK m.16, f.6)

SiGüK m.16, f.6, 1. cümlede düzenlenen siber saldırı suçu, Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren unsurlarına yönelik olarak siber saldırıda bulunan veya bu siber saldırı neticesinde elde edilen herhangi bir veriyi siber uzayda bulunduran kişilerin, sekiz yıldan on iki yıla kadar hapis cezası ile cezalandırılmasını öngörmektedir. Dolayısıyla suç, siber saldırı düzenlenmesi veya düzenlenen bir siber saldırı sayesinde elde edilen verilerin siber uzayda bulundurulması şeklinde iki ayrı seçimlik hareket ile işlenebilir. Failin somut olayda her iki seçimlik hareketi de icra etmesi durumunda yine tek suç oluşur. Ancak faile alt sınırdan uzaklaşarak ceza tayin edilir⁴¹.

Suçun seçimlik hareketlerinden ilki, siber saldırıda bulunmaktır. Kanun, hem siber saldırı hem de siber tehdit kavramlarını tanımlamıştır. Buna göre siber tehdit, bilişim sistemlerinin, bu sistemlerde bulunan veya bu sistemler tarafından işlenen verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesine neden olabilecek potansiyel tehlikeleri ifade eder (SiGüK m.3, f.1-h). Suçun seçimlik hareketini oluşturan siber saldırı ise siber uzaydaki bilişim sistemlerinin ve bu sistemler tarafından işlenen verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla siber uzayın herhangi bir yerindeki kişi veya bilişim sistemlerine yönelik olarak kasıtlı yapılan işlemler olarak tanımlanmıştır (SiGüK m.3, f.1-ğ). Siber saldırı, bilişim sistemlerini kullanım dışı bırakmak, verileri çalmak, değiştirmek, yok etmek gibi amaçlarla bilişim sistemlerinin açıklarını veya bu amaçla geliştirilmiş yazılımları kullanmak suretiyle bilişim sistemlerine yetkisiz erişim sağlanması suretiyle gerçekleştirilir⁴². Bu saldırılar, kişisel sebepler ile ekonomik çıkar amacıyla siyasi amaçlarla terör amacıyla ve devletler arası mücadelede siber savaş amacıyla yapılabilir. En bilinen siber saldırı yöntemleri, oltalama (phishing), dağıtılmış hizmet engelleme (ddos), ortadaki adam saldırısı, SQL enjeksiyonu, XXS güvenlik açığı, kaba kuvvet saldırıları, şifre saldırıları,

³⁹ Şenol (n9) 334.

⁴⁰ Özgenç (n3) 184, 191.

⁴¹ Koca, Üzülmüş (n13) 124; Artuk, Gökçen, Alşahin, Çakır (n2) 336.

⁴² Ebru Yıldırım Yeniman, "Bilişim Sistemlerine Yönelik Siber Saldırı ve Siber Güvenliğin Sağlanması", (2018) 7(2) *Mesleki Bilimler Dergisi*, 3.

fidye yazılımları, sıfır gün saldırısı, gelişmiş kalıcı tehdit (APT) olarak kabul edilmektedir⁴³. Örneğin, bir ülkenin elektrik veya doğalgaz hatlarının işletilmesini sağlayan bilişim sistemlerinin devre dışı bırakılması suretiyle enerji hatlarının devre dışı bırakılması, finans, ulusal güvenlik ve savunma sanayi alanında faaliyet gösteren kurumlara yönelik, bu kurumların elindeki bilgileri bulundukları bilişim sistemine uzun süreli olarak yerleşerek ele geçirmeye yönelik APT saldırıları ya da önemli kurumların web sitelerine ulaşılmasını engellemek için yapılan hacklemeler, siber saldırıya örnek verilebilir.

SiGüK m.3, f.1-ğ’de siber saldırı kavramı tanımlanırken siber uzayın herhangi bir yerindeki bilişim sistemleri dışında kişilere yönelik kasıtlı işlemlerin de siber saldırı olarak kabul edileceği düzenlemiştir. Buradaki kişiler ibaresi, bir şeyin siber saldırı olarak kabul edilebilmesi için saldırının siber uzayda gerçekleşmiş olması zorunluluğunun bulunduğundan da anlaşılacağı üzere kişilerin fiziksel varlıklarını değil, bireylere ait bilişim sistemlerini ifade eder. Zira Kanun siber uzayı, Doğrudan ya da dolaylı olarak internete, elektronik haberleşme veya bilgisayar ağlarına bağlı olan tüm bilişim sistemlerini ve bunları birbirine bağlayan ağlardan oluşan ortam olarak tanımlamıştır (SiGüK m.3, f.1-i). Dolayısıyla bu ifade ile kamu veya özel hukuk tüzel kişilerine ait bilişim sistemleri dışında gerçek kişilere ait sistemlerin de siber saldırı suçunun konusunu oluşturabileceğinin kabul edildiğini söylemek doğru olur. Bir kişiye ait akıllı telefona casus yazılım yerleştirilerek telefonun kontrolünün ele geçirilmesi ve verilerinin gizliliğinin ihlal edilmesi bu duruma örnek verilebilir.

SiGüK m.16, f.6, 1. cümlede Türkiye Cumhuriyeti’nin siber uzaydaki milli gücünü meydana getiren unsurlarına yönelik saldırıların siber saldırı suçunu oluşturacağı ifade edilmiştir. Söz konusu ifade, ilk bakışta kamu kurum ve kuruluşları ile ilgili olmayan özel hukuk gerçek ve tüzel kişilerine ait bilişim sistemlerinin siber saldırı suçunu oluşturmayacağı intibayı uyandırmaktadır. Ancak Kanun’un 1. maddesinde amacı belirtilirken “Türkiye Cumhuriyeti’nin siber uzaydaki milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel tehditlerin tespit ve bertaraf edilmesi...”’nden bahsedildikten sonra, kamu kurum ve kuruluşlarının yanı sıra kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşların da siber saldırılara karşı korunmasına yönelik gerekli düzenlemelerin yapılması zikredilmek suretiyle açıkça hem özel hukuk gerçek ve tüzel kişilerine ait bilişim sistemlerinin Türkiye Cumhuriyeti’nin siber uzaydaki milli güç unsurları arasında olduğu hem de bu kişilerin siber saldırılara karşı korunmasının Kanun’un amaçları arasında bulunduğu belirtilmiştir.

Siber saldırı suçu, bir yasak normunun ihlaliyle gerçekleştiği için icrai hareketli bir suçtur⁴⁴. Suçun icrası saldırı fiilinin gerçekleştirilmesiyle tamamlanıp

⁴³ Akbulut (n11) 72; Yeniman Yıldırım (n41) 3.

⁴⁴ Artuk, Gökçen, Alşahin, Çakır (n2) 337.



bitebileceği gibi bitmeden devam da edebilir. Bu sebeple hem ani hem mütemadi olarak işlenebilir⁴⁵. Örneğin, bir kişinin telefonunun casus yazılım yerleştirilerek takip edilmesi durumunda suç mütemadi, bilişim sistemine izinsiz girilerek belli verilerin yok edilmesi durumunda ani hareketli olarak işlenmiş olur. Siber saldırı seçimlik hareketinin oluşması için saldırı sonucunda bilişim sisteminin zarar görmesi, işlemez hale gelmesi, veri çalınması gibi bir sonuç veya bunlar üzerinde bir tehlike meydana gelmesi aranmamıştır. Dolayısıyla suç, bir soyut tehlike suçudur⁴⁶. Ancak siber saldırı fiili neticesinde çoğu durumda bir zarar meydana geleceği açıktır. Kanun koyucunun bir zarara yol açılmasını nitelikli hal veya neticesi sebebiyle ağırlaştırılmış hali olarak düzenlememiş olması, önemli bir eksiklik teşkil etmektedir. Mevcut durumda bu husus, ancak TCK m.61, f.1-e gereğince temel cezanın alt sınırdan uzaklaşarak belirlenmesine neden olabilir.

Suçu oluşturan ikinci seçimlik hareket, siber saldırıda bulunan kişilerin siber saldırı neticesinde elde ettikleri herhangi bir veriyi siber uzayda bulundurmasıdır. Öncelikle suçun bu seçimlik hareketinin ilk seçimlik hareketinden tamamen farklı olduğunu, dolayısıyla ayrı suç tipleri olarak düzenlemelerinin gerektiğini, hatta doğrusu suçun ikinci seçimlik hareketinin fıkranın ikinci cümlesinde düzenlenen ve konu unsuru aynı olan siber saldırı sonucunda elde edilen verinin yayılması suçunun seçimlik hareketlerinden biri olarak düzenlemesinin daha doğru olacağını belirtmek gerekir.

Siber saldırı neticesinde elde edilen verinin siber uzayda bulundurulması seçimlik hareketinin oluşması için suçun konusunu oluşturan elde bulundurulan verinin fail veya failler tarafından gerçekleştirdikleri siber saldırı neticesinde elde edilmiş bir veri olması gerektiğinden, failin öncesinde siber saldırı suçu işlemesi bu seçimlik hareket açısından önkoşul niteliğindedir. İkinci olarak bu siber saldırı sonucunda siber uzayda bulunan bir kısım veriler ele geçirilmiş olmalıdır. Üçüncü olarak da bu verileri ele geçirmiş kişiler, verileri siber uzayda bulundurmalıdır. Bulundurmak, bir şeyi fiili hakimiyeti, kontrolü altında tutma anlamına gelir⁴⁷. Dolayısıyla bulundurma seçimlik hareketinin oluşması için, failin, veriyi, üzerinde istediğinde tasarruf edebileceği şekilde fiili hakimiyeti ve kontrolü altında tutması gerekir⁴⁸. Örneğin, bir şirketin veritabanlarına yönelik icra edilen siber saldırı sonucunda elde edilen müşterilerin kişisel verilerinin bir bulut sisteminde depo edilmesi durumunda bu seçimlik hareket oluşur. Buna karşılık siber uzaya dahil olmayan bir taşınabilir hardisk veya usb bellek içerisinde bulundurulması durumunda bu suç oluşmaz.

⁴⁵ Özbek, Doğan, Bacaksız (n7) 239.

⁴⁶ Özgenç (n3) 221.

⁴⁷ Yamaner Özdemir n(30) 79.

⁴⁸ Yamaner Özdemir n(30) 79.

Suçun oluşması için bulundurma fiilinin üzerinde icra edileceği verilerin mutlaka kişisel veri niteliğinde olması aranmamış, veri olması yeterli sayılmıştır. Bu sebeple bir bilişim sistemi tarafından işlenen, bir şeyleri analiz etmekte kullanılan veya depolanan, sayılar, metinler, görüntüler, videolar, sesler ve başkaca herhangi bir formatta bulunan her şey veri kavramının kapsamına girer⁴⁹. Suçun oluşması için bu verilerin siber uzayda bir süre fiili hakimiyet altında tutulması yeterlidir. Bu sebeple suç, icrai hareketle mütemadi olarak işlenebilecek bir suçtur⁵⁰. Suçun oluşması için verilerin bulundurulması nedeniyle bir tehlike veya zarar ortaya çıkması aranmadığı için de soyut tehlike suçudur⁵¹.

G. SİBER SALDIRI SONUCUNDA ELDE ETTİĞİ VERİYİ YAYMA SUÇU (SiGüK m.16, f.6)

Kanun koyucu SiGüK m.16, f.6, ikinci cümlede, birinci cümlede yer verdiğinden farklı bir suç tip yaratarak gerçekleştirdiği siber saldırı neticesinde elde ettiği her türlü veriyi siber uzayda yayan, başka bir yere gönderen veya satışa çıkaranlara on yıldan onbeş yıla kadar hapis cezası verilmesi öngörülmüştür. Bu suçun konu unsuru, ilk cümlede düzenlenen verilerin bulundurulması suçuna ile aynı olduğu için veri kavramına ilişkin olarak yukarıda yapılan açıklamalar burası için de geçerlidir.

SiGüK m.16, f.6, ikinci cümlede düzenlenen suçun oluşması için, aynı verilerin bulundurulması suçunda olduğu gibi, faillerin önce siber saldırı suçunu işlemesi ve bu saldırı neticesinde siber uzayda bulunan bazı verileri ele geçirmesi gerekir. Bu durum, suçun oluşması için ön şart niteliğindedir.

SiGüK m.16, f.6, ikinci cümlede düzenlenen suçun fiil unsuru, siber saldırı neticesinde elde edilen verilerin siber uzayda yayılması, başka bir yere gönderilmesi veya satışa çıkarılmasıdır. Bu bakımdan suç, üç ayrı seçimlik hareketten birinin icrasıyla işlenebilecek seçimlik hareketli bir suçtur. Failin somut olayda seçimlik hareketlerden birden fazlasını icra etmesi durumunda yine tek suç oluşur. Ancak faile alt sınırdan uzaklaşılarak ceza tayini yoluna gidilir⁵².

Suçun fiil unsurunu oluşturan seçimlik hareketlerden ilki, siber saldırı neticesinde elde edilen verilerin siber uzayda yayılmasıdır. Bir veriyi yaymak, söz konusu verinin birden çok kişinin haberdar olabileceği veya erişebileceği şekilde paylaşılmasıdır⁵³. Yayma fiilinin gerçekleşmesi için failin siber saldırı neticesinde elde ettiği veriyi birden çok kişinin haberdar olabileceği şekilde ulaşılabilir

⁴⁹ Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil*, (Seçkin Yayıncılık, Ankara 2014) 50 vd; Akbulut (n11) 188.

⁵⁰ Zafer (n27) 262.

⁵¹ Özgenç (n3) 221.

⁵² Koca, Üzülmöz (n13) 124; Artuk, Gökçen, Alşahin, Çakır (n2) 336.

⁵³ Bayraktar (n29) 642.



kılması yeterlidir. Yaymanın ne şekilde gerçekleştirildiği suçun oluşması bakımından önem taşımaz. Veri, yazılı, sesli veya görüntülü bir veri olabilir ve bu şekilde yayılabilir. Yayma fiilinin gerçekleşmiş sayılması için yayılan bilginin birden çok kişi tarafından öğrenilmesi de gerekmez. Önemli olan siber uzayda başkaları tarafından öğrenilebilecek şekilde paylaşılmasıdır⁵⁴. Yaymanın siber uzay kavramına dahil olmayan fiziksel şekilde yayılması durumunda bu suç oluşmaz. Bu sebeple bir gazete, dergi ya da kitapta basılması bu suçu oluşturmaz.

Suçun diğer seçimlik hareketi olan siber saldırı neticesinde elde edilen verilerin aslının ya da kopyasının siber uzayda başka bir yere gönderilmesi, verilerin siber uzayda bulunan bir bilişim sistemi veya bunların bağlı olduğu ağlarda bir yerden başka bir yere nakledilmesidir⁵⁵. Gönderme, yaymadan farklı olarak verinin başka kişiler tarafından öğrenilmesini değil, verinin veriyi elde edenin güvenli bir biçimde kontrol edebilmesi için başka bir bilişim sistemine veya sistemin parçası olduğu ağ içerisinde daha güvenli gördüğü bir yere aktarılmasını ifade eder. Bu bakımdan gönderme, siber saldırı sonucunda elde edilen veriler üzerindeki hakimiyetin sürdürülmesi için yapılır⁵⁶.

Suçun üçüncü seçimlik hareketi, siber saldırı neticesinde elde edilen verilerin siber uzayda satışa çıkarılmasıdır. Verinin satışa çıkarılması, verinin zilyedi olan veya en azından istediğinde erişebilecek durumda olan kişilerin, ücret karşılığı veriyi bir başkasına devretme iradesini gösteren, satmaya yönelik ve satmadan önce gelen tüm hareketlerini ifade eder⁵⁷. Müşteri arama, bir ekonomik menfaat karşılığı anlaşmaya çalışma gibi hareketler, bu seçimlik hareketi oluşturur. Bu seçimlik hareketin oluşması için verinin siber uzayda satışa çıkarılması gerekir. Fiziki ortamda satışa çıkarma, suçun bu seçimlik hareketine vücut vermez.

Suçun her üç seçimlik hareketi de işlenme biçimleri konusunda herhangi bir sınırlamaya gidilmediği için serbest hareketli, bir yasak normunun icrasıyla işlenebileceği için icrai hareketli ve işlenmeleri neticesinde herhangi bir zarar veya tehlikenin ortaya çıkması aranmadığı için soyut tehlike suçu niteliğindedir⁵⁸. Seçimlik hareketlerden bulundurma ve satışa çıkarma mütemadi hareketli; gönderme, göndermenin gerçekleşmesi ile suç hem tamamlanıp hem de biteceği için ani hareketlidir.

H. YASAK HÜKÜMLERE AYKIRI DAVRANMA SUÇU (SiGüK m.16, f.8)

SiGüK m.16, f.8'de düzenlenen yasak hükümlere aykırı davranma suçu, Kanun'un 12. maddesinde Siber Güvenlik Başkanlığında kadrolu veya sözleşmeli

⁵⁴ Şenol (n9) 334.

⁵⁵ Akbulut (n2) 202.

⁵⁶ Akbulut (n2) 202.

⁵⁷ Yamaner Özdemir (n30) 69.

⁵⁸ Zafer (n27) 256; Karakehy (n3) 61.

statüde çalışmış kişiler için getirilmiş bazı davranış yükümlülüklerine aykırı davranılmasını suç olarak düzenlenmiştir. Suç bu bakımdan belli kişiler tarafından, Kanun ile yasaklanmış bazı davranışlara aykırı davranılması ile işlenebileceği için icrai hareketli bir suçtur⁵⁹.

SiGüK 12. maddesinde düzenlenen yasak fiillerin ilk grubu, söz konusu maddenin 1. fıkrası gereğince başkanlık bünyesinde kadrolu veya sözleşmeli statüde çalışmış ve istifa, işten çıkarma gibi herhangi bir sebeple kurumdan ayrılmış personelin iki yıl süreyle Başkanlıktan muvafakat almadan, siber güvenlik alanında herhangi bir sıfatla çalışması ve faaliyette bulunmasıdır. Yasaklanan bu hususlar fıkra, siber güvenlik alanında a) resmi veya özel görev alma, b) ticaretle uğraşma, serbest meslek faaliyetinde bulunma ve bu kapsamda bu sektörde faaliyet gösteren bir şirkette hissedar veya yönetici olma şeklinde sayılmıştır. Dolayısıyla bu fıkra açısından suç teşkil eden fiil aslında faaliyette bulunma değil, Başkanlığın muvafakati olmadan faaliyette bulunmadır. Bu bakımdan suç, bağlı hareketli bir suçtur⁶⁰. Örneğin, Başkanlıktan istifa etmiş bir personelin, Başkanlıktan muvafakat almadan, siber güvenlik alanında faaliyet gösteren bir siber güvenlik şirketinde veya örneğin bir şirketin bilişim sistemlerinin siber güvenliğinden sorumlu bilgi işlem servisinde çalışması ya da böylesi bir şirkete danışmanlık hizmeti vermesi durumunda söz konusu suç oluşur.

SiGüK m.12, f.2’de düzenlenen yasak fiillerin ikinci grubu ise çalışan veya görevden ayrılan personelin, Başkanlıkça yetki verilmedikçe, icra ettikleri görev ve faaliyetleri kapsamında edindiği bilgi, belge ve benzeri her türlü veriyi radyo, televizyon, internet, sosyal medya, gazete, dergi, kitap ve diğer tüm medya araçları ile her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim araçları vasıtasıyla yayımlanması veya açıklanmasıdır. Dolayısıyla suçun bu seçimlik hareketi, Başkanlık personeli tarafından görevi gereği öğrenilen suçun konusunu oluşturan bilgi, belge veya verilerin herhangi bir şekilde yayımlanması veya açıklanması, yani başka kişilerce öğrenilmesine imkân sağlanması ile oluşur. Ancak hiç kuşkusuz burada suçun oluşabilmesi için, açıklama ve yayma fiilinin konusunu oluşturan bilgi, belge ve verilerin, SiGüK m.16, f.3’te düzenlenen ve daha özel norm niteliğinde olan sır saklama yükümlülüğünün ihlali suçunun kapsamına giren Kanun’un 13. maddesinde sır saklama yükümlülüğü kapsamında gördüğü, *“kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgiler, kişisel veriler, ticari sırlar ve bunlara ait belgeler”* den olmaması gerekir. Bu sebeple gizlilik niteliğine haiz bir siber savaş anında yapılacak işleri içeren belgeler, bu suçun değil, sır saklama yükümlülüğünün ihlali suçunun konusunu oluşturur. Buna karşın gizlilik vasfı olmayan bir siber saldırıya ilişkin kamuoyunca bilinmeyen ve Başkanlık çalışanının görevi gereğince öğrendiği bilgi, bu suçun konusunu oluşturur.

⁵⁹ Artuk, Gökçen, Alşahin, Çakır (n2) 337.

⁶⁰ Özbek, Doğan, Bacaksız (n7) 235.



Yayımlanma veya açıklanma fiilinin oluştuğundan bahsedilebilmesi için, bilgi veya belgenin, kendisine gizli olan en az bir kişinin öğrenebileceği şekilde aktarılması yeterlidir. Açıklama fiilinin tamamlanması için muhatabın açıklanan bilgi veya belgeyi öğrenmesi gerekmez, failin bilgi veya belgeyi öğrenmeye elverişli şekilde aktarmasıyla fiil tamamlanmış olur⁶¹. Ancak bilginin veya belgenin açıklandığından bahsedilebilmesi için, suçla korunan hukuki değeri ihlal edebilecek en azından bir kısmının içerik olarak başka kişi veya kişilere iletilmesi gerekir. İçeriğini açıklamadan sadece bilgi veya belgenin varlığının bildirilmesi, açıklama fiilini oluşturmaz⁶². Örneğin, Türkiye'ye yönelik bir siber saldırı gerçekleştiğine ilişkin, saldırının herhangi bir ayrıntısını içermeyen bir telefon mesajı, açıklama içermediği için suç oluşturmaz. Buna karşın böylesi bir saldırıya ilişkin bilgileri içeren gizlilik vasfı olmayan bir kurum raporunun bir gazeteciye gönderilmesi, bu suç oluşturmaz. Suç, kanuni tanımında bu seçimlik hareketinin ne şekilde işleneceği konusunda herhangi bir sınırlamaya gidilmemek suretiyle bilgi, belge veya verinin yazılı, sözlü, görsel, işitsel herhangi bir şekilde yayımlanması veya açıklanması ile işlenebileceği kabul edildiği için, serbest hareketli bir suçtur⁶³.

I. GÖREVİ VE YETKİYİ KÖTÜYE KULLANMA SUÇU (SiGüK m.16, f.9)

Siber Güvenlik Kanunu'nda düzenlenen dokuzuncu ve sonuncu suç, görevi ve yetkiyi kötüye kullanma suçudur. Kanun koyucu, muhtemelen TCK m.257'de düzenlenen görevi kötüye kullanma suçundan esinlenerek bu Kanun açısından da bir görevi kötüye kullanma suçu ihdas etmiş, bunu yaparken de SiGüK'nde düzenlenen birçok suç tipi gibi bu suçu da seçimlik hareketli suç olarak düzenlenmiştir. Buna göre mezkûr suç, SiGüK'nden kaynaklanan görev ve yetkilerini kötüye kullanılması veya kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket edilmesi suretiyle veri ihlali yaşanmasına sebebiyet verilmesi şeklinde iki ayrı seçimlik hareketin icrasıyla işlenebilir. Suçun iki seçimlik hareketinin birlikte işlendiği veya Kanun'dan kaynaklanan görev ve yetkinin kötüye kullanılmasının kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket etme de teşkil ettiği durumlarda, tek suç oluşur. Ancak bu durum, TCK m.61 gereğince temel cezanın alt sınırından uzaklaşarak belirlenmesini gerektirir⁶⁴.

Suçun seçimlik hareketlerinden ilki olan bu Kanun'dan kaynaklanan görev ve yetkinin kötüye kullanılmasının oluşması için, Kanun kapsamında görevlendirilmiş SGB çalışanları veya SGB'nin verdiği yetki ile faaliyet gösteren kişi ve kurumların, Kanunen kendisine tanınan görev ve yetkileri kötüye kullanması ge-

⁶¹ Tezcan, Erdem, Önok (n21) 702; Koca, Üzülmüş (n21) 576.

⁶² Tezcan, Erdem, Önok (n21) 702; Koca, Üzülmüş (n21) 576.

⁶³ Özgenç (n3) 184; Karakehya (n3) 56.

⁶⁴ Artuk, Gökçen, Alşahin, Çakır (n2) 336; Koca, Üzülmüş (n13) 124.

rekir. Bu kapsamda suçun oluşması için öncelikle fail, SiGüK’nden kaynaklanan bir görev ve yetkiye sahip olmalıdır. Bu sebeple failin yaptığı eylemler kendisinin değil de örneğin SGB’de çalışan başka bir çalışanın görevine giriyorsa bu suç oluşmaz⁶⁵. İkinci olarak da fail görev ve yetkisinin kapsamına giren bir durumda, icrai bir davranışla yapması yasaklanan bir şeyi yapmalı veya emredilen bir şeyi yapmamış olmalıdır. Bu bakımdan görevin gereklerine aykırı hareket, hem icrai hem ihmalî hem ani hem mütemadi olarak işlenebilecek serbest hareketli bir suçtur⁶⁶. Suçun oluşması veya faile ceza verilebilmesi için, görev ve yetkinin kötüye kullanılması sonucunda, örneğin kamunun zarara uğraması veya bireylerin mağduriyet yaşaması gibi herhangi bir zarar veya zarar tehlikesinin ortaya çıkması aranmadığı için, suçun bu seçimlik hareketi, soyut tehlike suçu olarak düzenlenmiştir. SGB bünyesinde çalışan personelin 5237 sayılı TCK m.6, f.1-c gereğince kamu görevlisi olduğu göz önünde bulundurulduğunda, kanun koyucunun böylesi bir koşulun arandığı TCK m.257’ye göre⁶⁷ özel norm niteliğinde olacak böylesi bir suç tipini farklı tipiklik unsurları arayarak yaratmasının gerekli ve isabetli olmadığını belirtmek gerekir.

Suçun ikinci seçimlik hareketi, kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket edilmesi suretiyle veri ihlali yaşanmasına sebebiyet verilmesidir. Bu seçimlik hareketin oluşması için, SiGüK m.3, f.1-d’de kritik altyapı olarak tanımlanan *“İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara ve güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar”*a yönelik bir siber saldırıda bulunulmalıdır. Dolayısıyla herhangi bir siber saldırı değil, sadece sağlık sistemi, ulaşım sistemi, su tedarik altyapısı, borsa, merkez bankası gibi önemli finansal kurumlar, savunma ve güvenlik birimleri gibi kritik altyapılara yönelik ciddi ölçekteki siber saldırılar sırasında görevin gereklerine aykırı hareket edilmesi bu seçimlik harekete vücut verir. Buna karşın siber uzayda kritik alt yapı niteliğinde olmayan yerlere yapılan siber saldırılar sırasında görevin gereklerine aykırı hareket edilmesi, suçun ilk seçimlik hareketini oluşturur. Suçun bu seçimlik hareketinin oluşması için ikinci koşul, failin kritik nitelikteki altyapılara yönelik bir siber saldırı sırasında görevin gereklerine aykırı hareket etmesidir⁶⁸.

⁶⁵ Yokuş Sevik (n10) 270; Okuyucu Ergün (n10) 7; Mehmet Emin Artuk, Ahmet Gökçen, M. Emin Alşahin, Kerim Çakır, *Ceza Hukuku Özel Hükümler*, (20. Baskı, Adalet Yayınevi, Ankara 2022) 1132.

⁶⁶ Yokuş Sevik (n10) 268 vd; Okuyucu Ergün (n10) 7 vd.

⁶⁷ Söz konusu koşul için bakınız: Yokuş Sevik (n10) 282.

⁶⁸ Öğretide belirtildiği üzere kamu görevlileri açısından görevin gereklerinin nelerden ibaret olduğu, kanun, idari düzenlemeler, mesleki uzmanlık bilgisi ve gelenekler ile belirlenir. Bu sebeple söz konusu ifadenin aslında bir açık ceza normu olduğu da ileri sürülmüştür. Somut bir davada bu durum, büyük ölçüde bilirkişi incelemesi ve SGB denetim raporları ile belirlenebilecektir. Görevin gereklerine aykırı hareket için bakınız: Okuyucu Ergün, (n10) 6 vd.



Örneğin, failin, siber saldırıyı gerçekleştirenler ile birlikte hareket ederek siber savunma önlemlerini devre dışı bırakması ya da sistemin siber saldırı uyarısına rağmen hareketsiz kalarak siber saldırıyı püskürtmek veya verilerin güvenliğini temin etmek için gerekenleri yapmaması durumunda bu seçimlik hareket oluşur. Dolayısıyla suçun bu seçimlik hareketi de hem icrai veya ihmali hem ani ya da mütemadi olarak işlenebilir. Ancak kanun koyucu, suçun ilk seçimlik hareketinin aksine bu seçimlik hareketinin oluşmasını için görevin gereklerine aykırı hareket edilmesinin veri ihlaline sebebiyet vermesi şeklinde bir neticeye yol açmasını aramış; dolayısıyla bu seçimlik hareketi, neticeli suç olarak düzenlemiştir. Bu sebeple failin suçun bu seçimlik hareketinden cezalandırılabilmesi için, kritik altyapılara yönelik siber saldırıların savunulmasına ilişkin bir görevinin olması, bu görevin gereklerine aykırı icrai veya ihmali bir davranışı bilerek yapması veya yapmaması, failin görevin gereklerine aykırı hareketinin veri ihlali yaşanmasına neden olması, yani veri ihlali ile failin görevin gereklerine aykırı hareketi arasında nedensellik bağı bulunması ve veri ihlali yaşanmasının faile objektif olarak isnad edilebilmesi gerekir. Veri ihlali yaşanmasının faile objektif olarak isnad edilmediği durumlarda suç da oluşmaz⁶⁹. Ancak bu seçimlik harekette veri ihlali sebebiyet vermenin bir objektif cezalandırma şartı olarak düzenlenmesinin daha doğru olacağını belirtmek gerekir.

V. KONU

Suçun konusu, suç teşkil eden fiilin yöneldiği kişi veya şeydir⁷⁰. SiGüK m.16'da düzenlenen farklı suç tipleri, konu unsuru bakımından da farklılık göstermektedir.

SiGüK m.16, f.1'de düzenlenen kanunla yetkilendirilen mercilerin ve denetim görevlilerinin görev ve yetkileri kapsamında istedikleri bilgi, belge, yazılım, veri ve donanımı vermeme veya bunların alınmasına engel olma suçunun konusu, verilmeyen veya alınmasına engel olunan bilgi, belge, yazılım, veri ve donanımdır. Ancak suçun konusu, kamu kurum ve kuruluşları hariç Kanun'un kapsamına giren kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşlara ait bilgi, belge, yazılım, veri ve donanım ile sınırlanmıştır. Bu sebeple kamu kurum ve kuruluşlarına ait olanlar, suçun konusunu oluşturmaz.

SiGüK m.16, f.2'de düzenlenen kanunen alınması gerekli onay, yetki veya izinleri almaksızın faaliyet yürütme suçunun konusu, gerekli onay veya izin alınmaksızın siber güvenlik alanında yürütülen faaliyetlerdir. Dolayısıyla bu fıkarda düzenlenen suçun fiil unsuru faaliyetin gerekli onay, yetki veya izni olmadan yürütülmesi, konusu ise izinsiz olarak yürütülen faaliyettir.

⁶⁹ Koca, Üzülmüş (n13) 140.

⁷⁰ Zafer (n27) 208; Hakeri (n7) 144.

SiGüK m.16, f.3'te düzenlenen sır saklama yükümlülüğünün ihlali suçunun konusu, Kanun'un 13. maddesi gereğince açıklanması veya gerçek ya da tüzel kişilerin menfaatine kullanılması yasak olan ve Başkanlık tarafından yürütülen görev ve faaliyetler kapsamında edinilen kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgiler, kişisel veriler, ticari sırlar ve bunlara ait belgelerdir.

SiGüK m.16, f.4'te düzenlenen sızıntı sonucu oluşan verileri erişime açma, paylaşma ve satışa çıkarma suçunun konusu, erişime açılması, paylaşılması, satışa çıkarılması bu fıkra düzenlenmiş suç ile yasaklanmış, siber uzayda veri sızıntısı nedeniyle daha önce yer alan kişisel veriler ile kritik kamu hizmetiyle ilgili kurumsal verilerdir. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir⁷¹. Kritik kamu hizmeti SiGüK m.3, f.1-e'de ulusal, toplumsal veya ekonomik faaliyetlerin sürdürülmesi için gerekli olan ve kesintiye uğraması veya zarar görmesi halinde ulusal güvenlik, ülkenin sosyal veya ekonomik refahı, kamu düzeni veya sağlığı ya da diğer hizmetlerin sunumu üzerinde önemli bir etki oluşturabilecek ülke genelinde tekel veya sınırlı ikame ile sunulan hizmet olarak tanımlanmıştır. Dolayısıyla kritik kamu hizmetine ilişkin veri, belirtilen nitelikteki hizmetleri yürüten kurumlara ilişkin her türlü veriyi ifade eder. Örneğin, sağlık hizmetleri, toplumsal faaliyetlerin sürdürülmesi için gerekli ve kesintiye uğraması veya zarar görmesi kamu sağlığını hatta diğer hizmetlerin sunumunu önemli ölçüde etkileyebilecek bir hizmet olduğu için, kritik bir kamu hizmetidir. Aynı şekilde ulaştırma, enerji, güvenlik, bankacılık gibi hizmetler, anılan özellikte olduğu için kritik kamu hizmetidir. Bu sebeple hizmeti yürüten kuruluşların söz konusu hizmetlere ilişkin verileri, bu suçun konusunu oluşturur. Burada suçun konusunu oluşturan veri, sadece örneğin E Nabız uygulamasında yer alan veriler gibi özellikli veriler değil, kamu sağlığı ile ilgili kritik kamu hizmeti kapsamındaki tüm verilerdir. Zira kanun koyucu bir verinin bu suçun konusunu oluşturabilmesi için kritik nitelikte olmasını aramamış, kritik kamu hizmetine ilişkin olmasını yeterli görmüştür. Bu sebeple Sağlık Bakanlığına ait, sağlık hizmetlerinin görülmesine ilişkin tüm veriler bu suçun konusunu oluşturabilir. Ancak sağlık hizmetlerinin görülmesine ilişkin olmayan veriler, bu suçun konusunu oluşturmaz. Yine kritik kamu hizmeti, ülke genelinde tekel veya sınırlı ikame ile sunulan hizmet olarak tanımlandığı için, bu nitelikte olmayan kurumlara ilişkin veriler suçun konusunu oluşturmaz. Örneğin, bir şehirde tekel olarak işletilen metro ve tramvay gibi ulaştırma hizmetlerine ya da su kanalizasyon hizmetlerine ilişkin kurumların sunduğu hizmet tekel niteliğinde olduğu için, bu suçun konusunu oluşturur. THY gibi sınırlı ikamesi olan kurum ve kuruluşlara ilişkin veriler de bu suçun konusunu oluşturur. Buna karşın sınırlı ikamesi olduğu kabul edilemeyecek bir özel bankaya ilişkin verilerin bu suçun

⁷¹ Oğuz Usta, *Kişilik Hakkı Bağlamında Unutulma Hakkı*, (Adalet Yayınevi, Ankara 2023) 53; Bahar Turgut, "Türk Ceza Hukukunda Verileri Yok Etmeme Suçu (TCK m.138)", (Mart 2025) (233) *Terazi Hukuk Dergisi*, 133.



konusunu oluşturmadığını kabul etmek daha doğru olur. Zira gerçek kişi vasfında olmayan siber uzayda varlık gösteren, faaliyet yürüten, hizmet sunan kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşlara ait veriler, kritik kamu hizmetine ilişkin olmadığı sürece bu suçun konusunu oluşturmaz.

SiGüK m.16, f.5'te düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma ve yayma suçunun konusu, oluşturulması ve yayılması suç olarak düzenlenmiş veri sızıntısı gerçekleştiği hakkındaki gerçeğe aykırı içeriklerdir. Suçun konusunu oluşturan içerikler görsel, yazılı, sözlü olabilir. Örneğin, gerçekleşmemiş bir siber saldırı sonucu belli bir sitenin üyelerinin kişisel bilgilerinin çalındığını gösteren sahte ekran görüntüleri veya böylesi bir durumun gerçekleştiğini iddia eden gizli ses ya da röportaj kaydı suçun konusunu oluşturur.

SiGüK m.16, f.6'nın birinci cümlesinde düzenlenen siber saldırı suçunun konusu, siber saldırı teşkil eden kasıtlı işlemlerin kendisine karşı gerçekleştirildiği, siber uzayın herhangi bir yerindeki kişi veya bilişim sistemleridir. Bu suç açısından suçun konusunu oluşturan bilişim sistemlerinde yer alan veriler de suçun konusuna dahildir.

SiGüK m.16, f.6'nın ikinci cümlesinde düzenlenen siber saldırı sonucunda elde edilen veriyi yayma suçunun konusu ise siber saldırı sonucu elde edildikten sonra yayılan verilerdir. Kanun koyucu, bu suçun konusunu oluşturabilecek verinin niteliği konusunda, kişisel veri olması, kritik bir kamu hizmetine ilişkin olması gibi herhangi bir sınırlamaya gitmemiştir. Dolayısıyla her türlü veri, suçun konusunu oluşturur. Bir bilişim sistemi tarafından işlenebilen ve depolanabilen, bir şeyleri analiz etmekte kullanılan sayılar, metinler, görüntüler, videolar, sesler ve başkaca herhangi bir formatta bulunan her şey, veri kavramının kapsamına girer⁷²

SiGüK m.16, f.8'de düzenlenen yasak hükümlere aykırı davranma suçunun konusu, Kanun'un 12. maddesinde Başkanlıkta kadrolu veya sözleşmeli statüde çalışmış ve herhangi bir nedenle ilişkisi kesilmiş kişilere izin alınmadan yapılması yasaklanan, iki yıl süreyle yurt içi veya yurt dışında siber güvenlik alanında resmi veya özel görev alma, siber güvenlik alanında ticaretle uğraşma, serbest meslek faaliyetinde bulunma, sektörde faaliyet gösteren bir şirkette hissedarlık veya yöneticilik yapma ile bu kişilerin Başkanlıktaki görevleri ve faaliyetleri kapsamında edindiği ve yayımlanması ve açıklanması yasaklanmış her türlü bilgi, belge ve benzeri veridir.

SiGüK m.16, f.9'da düzenlenen görevi ve yetkiyi kötüye kullanma suçunun konusu, suçun failinin kötüye kullandığı veya gereklerine aykırı hareket ettiği yetkisi ve görevidir. Bu yetki ve görevlerin neler olduğu, kanun, idari düzenlemeler ve meslek uzmanlık bilgisi ile belirlenir⁷³.

⁷² Değirmenci (n41) 50 vd.; Akbulut (n2) 188.

⁷³ Görev ve yetki konusunda bakınız: Yokuş Sevik, (n10) 270; Okuyucu Ergün (n10) 6 vd.

VI. NİTELİKLİ HALLER

SiGüK m.16, f.7’de, maddede düzenlenen suçlar için üç ayrı nitelikli hal belirlenmiştir. Nitelikli hale ilişkin düzenleme maddenin yedinci fıkrasında yapıldığı için, bu nitelikli hallerin 8. fıkra da düzenlenen yasak hükümlere aykırı davranma suçu ile 9. fıkrasında düzenlenen görevi ve yetkiyi kötüye kullanma ile görevin gereklerine aykırı hareket etmek suretiyle veri ihlaline sebebiyet verme suçlarına uygulanması mümkün değildir. Dolayısıyla suçun kamu görevlisi tarafından veya birden fazla kimse tarafından ya da bir örgüt faaliyeti çerçevesinde işlenmesi, Kanun’un 8. ve 9. fıkrasında düzenlenen suçlar haricinde kalan ilk altı fıkra da düzenlenen suçlar açısından cezanın ağırlaştırılmasını gerektiren nitelikli hal teşkil eder.

SiGüK m.16, f.7’de nitelikli hal olarak düzenlenen ilk hal, suçun kamu görevlisi tarafından işlenmesidir. Bu durumda işlenen suç nedeniyle verilecek cezanın üçte bir oranında artırılması öngörülmüştür. Kamu görevlisi deyimi, TCK m.6, f.1-c gereğince “*kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi*”yi ifade eder⁷⁴. Bu sebeple söz konusu nitelikli halin uygulanması için suçun SGB bünyesinde çalışan kişiler tarafından işlenmesi gerekli olmayıp TCK’nin uygulaması açısından kamu görevlisi sayılan herhangi bir kişi tarafından işlenmesi yeterlidir. Bu nitelikli halin 8. ve 9. fıkra da düzenlenen suçlar açısından kabul edilmemesi, söz konusu fıkralarda düzenlenen suçların failinin TCK m.6, f.1-c gereğince ceza kanunlarının uygulanması bakımından kamu görevlisi olan Başkanlık personeli olması nedeniyle isabetli; bunun aksine aynı durumun söz konusu olduğu 3. fıkra da düzenlenen sır saklama yükümlülüğünün ihlali suçunda uygulanmasının öngörülmesi ise oldukça hatalı olmuştur.

SiGüK m.16, f.7’de nitelikli hal olarak düzenlenen ikinci hal, suçun birden fazla kimse tarafından işlenmiş olmasıdır. Bu durumda suçun cezasının yarı oranında artırılması öngörülmüştür. Söz konusu nitelikli hal, TCK’de, m.79’da düzenlenen göçmen kaçakçılığı (TCK m.79, f3), m.102’de düzenlenen cinsel saldırı (m.102, f.3-d), m.148’de düzenlenen yağma (TCK m.149, f.1-c) suçları gibi birçok suçta nitelikli hal olarak düzenlemiştir. Bu nitelikli halden kasıt, suçun müşterek fail sıfatıyla en azından iki veya daha fazla kişi tarafından birlikte işlenmiş olmasıdır. He ne kadar 7. fıkra da, TCK’nin aksine “birlikte” işlenmesi ifadesine yer verilmemiş olsa da şerikler, suçun işleyen değil, sadece suçun icrasına maddi veya manevi katkı sağlayan kişiler olduğundan, suçu işleyen konumunda değildir. Bu sebeple mevzubahis nitelikli halin, tek bir failin suçunu birden fazla azmettiren

⁷⁴ Türk ceza kanununun uygulanması açısından kamu görevlisi kavramından ne anlaşılabileceği hakkında bakınız: Kaplan (n6) 61 vd.

veya yardım eden şerik ile iştirak halinde işlediği durumlarda uygulama alanı bulmayacağını kabul etmek isabetli olur⁷⁵.

SiGüK m.16, f.7'de nitelikli hal olarak düzenlenen üçüncü ve son hal ise maddede düzenlenen suçların bir örgütün faaliyeti çerçevesinde işlenmesidir. Bu durumda verilecek cezanın yarısından iki katına kadar artırılması öngörülmüş, böylece hâkime örgütün niteliğine göre farklı oranda artırım yapma yetkisi verilmiştir. TCK'de söz konusu halin nitelikli hal olarak kabul edildiği diğer suçlarda olduğu gibi burada da örgüt kavramından TCK m.220, f.1'de düzenlenen suç işlemek amacıyla örgüt kurma suçuna göre kurulmuş suç örgütleri anlaşılmalıdır⁷⁶. Ayrıca Türk hukukunda terör örgütlerinin cezalandırılmasının hukuki dayanağını TCK m.220 oluşturduğu için, fıkra düzenlenmiş örgüt kavramının kapsamına terör örgütleri de girer⁷⁷. Bu durumda suç, 3713 sayılı Terörle Mücadele Kanunu⁷⁸ (TMK) m.4 gereğince nispi terör suçu teşkil eder. TMK m.5'te bir suçun nispi terör suçu olarak düzenlenmesi durumunda cezanın yarı oranında artırılacağı kabul edilmiştir. SiGüK m.16, f.7'de ise bu durumda cezanın yarısından iki katına kadar artırılması öngörülmüştür. Bu sebeple artırımın özel ve sonraki norm niteliğinde olan bu fıkra gereğince yapılması gerekir⁷⁹. Bu nitelikli halin uygulanabilmesi için, örgüt suçu açısından aranan koşulların oluşması, ayrıca hem örgüt hakkında hem de fail veya failerin örgüte üyeliği hakkında verilmiş mahkûmiyet kararı bulunması gerekir⁸⁰.

Kanun koyucunun SiGüK'nda düzenlenen suçlar açısından fiilin işleniş şekli, ortaya çıkaracağı zarar veya tehlikenin ağırlığı, failin amacı, suçun işlendiği zaman gibi hususlara dair nitelikli haller belirlemediği görülmektedir. Bunun önemli bir eksiklik olduğunu söylemek mümkündür. Örneğin, siber saldırı suçun veya sır saklama yükümlülüğünün ihlali suçunun savaş zamanı işlenmesi, siber saldırı suçunun fidye yazılım uygulaması ile gerçekleştirilmesi gibi durumların nitelikli hal olarak düzenlenmesi isabetli olurdu. Mevcut düzenleme karşısında bu gibi

⁷⁵ Artuk, Gökçen, Alşahin, Çakır (n64) 623; Özen, Mustafa, Ceza Hukuku Özel Hükümler, (9. Baskı, Adalet Yayınevi, Ankara 2024), s.459.

⁷⁶ Tezcan, Erdem, Önok (n21) 103; Özbek, Doğan, Bacaksız (n26) 79. Bir topluluğun örgüt olup olmadığı, TCK m.220 uyarınca tespit edilir. TCK m.220 gereğince üye sayısının en az üç veya daha fazla kişi olması, üyeler arasında gevşek de olsa hiyerarşik bir bağ bulunması, suç işlemek amacıyla yönelik fiili bir birleşme bulunması, örgütün niteliği itibarıyla devamlılığının olması ve amaçlanan suçları işlemeye elverişli nitelik ve nicelikte üyeye, araç ve gerece sahip olması, son olarak da bu koşulların bir arada bulunması gerekir. Koşullardan birinin dâhi gerçekleşmemesi halinde suç işlemek amacıyla kurulmuş örgütten söz edilemez. **Yargıtay Ceza Genel Kurulu, E. 2014/9-718, K. 2016/5, 19.01.2016.**

⁷⁷ Tezcan, Erdem, Önok (n21) 103.

⁷⁸ 12.4.1991 tarihli ve 20843 sayılı mükerrer Resmî Gazete'de yayımlanmıştır.

⁷⁹ Tezcan, Erdem, Önok (n21) 103.

⁸⁰ Tezcan, Erdem, Önok (n21) 104.

hallerin ancak TCK m.60, f.1 gereğince temel cezanın alt ve üst sınırlar arasında belirlenmesi sırasında dikkate alınabileceğini belirtmek gerekir.

VII. MANEVİ UNSUR

TCK'ye göre suçun asıl manevi unsuru kast iken taksir istisnai işleniş biçimidir (TCK m.21, f1. ve m.22, f.1). Kast, kendi içinde doğrudan ve olası kast; taksir de basit ve bilinçli taksir olarak ikiye ayrılır. Bunun dışında suçun manevi unsurunun oluşması için, failin belli bir maksat veya saikle hareket etmesinin arandığı suçlar da bulunmaktadır⁸¹. Kanun koyucu, SiGüK m.16'da düzenlendiği dokuz farklı suçtan hiçbirisinin taksirle işlenmesi durumunda cezalandırılmasını öngörmemiştir. Bu sebeple Kanun'da düzenlenen suçların dikkat ve özen yükümlülüğünün ihlali ile işlenmesi durumunda cezalandırılabilmesi mümkün değildir (TCK m.22, f.1). Örneğin, bir kişinin sorumlu olduğu kritik kamu hizmetine ilişkin bir siber güvenlik sistemini dikkat ve özen yükümlülüğüne aykırı olarak devre dışı bırakması nedeniyle veri ihlali yaşanmasına neden olması durumunda, kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket etmek suretiyle veri ihlali yaşanmasına sebebiyet vermesine karşın kasten değil taksirle hareket ettiği için fiili suç teşkil etmez. Yine Başkanlık tarafından yürütülen görev ve faaliyetler kapsamında edindiği kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgiler, kişisel veriler, ticari sırlar ve bunlara ait belgeleri, başka belge sanıp dikkatsizlik sonucu örneğin cep telefonundan bir başkasına gönderen kişi, SiGüK m.16, f.3'te düzenlenen sır saklama yükümlülüğünün ihlali suçundan cezalandırılmaz.

SiGüK'nda düzenlenen suçlar içerisinde failin belli bir maksat veya saikle hareket etmesini gerektiren sadece bir suça yer verilmiştir. SiGüK m.16, f.5'te düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma suçunun manevi unsurunun oluşması için, failin, siber güvenlikle ilgili veri sızıntısı olduğuna yönelik gerçeğe aykırı içerik oluşturma veya bu maksatla bu içerikleri yayma şeklindeki seçimlik hareketleri, siber uzayda veri sızıntısı olmadığını bildiği halde halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef göstermek amacıyla oluşturmaya veya yaymaya aranmıştır⁸². Dolayısıyla söz konusu suç bir maksat suçu olup suçun oluşması için failin suçun konusunu oluşturan içeriklerin gerçeğe aykırı olduklarını bilmesi ve iradesini bu içerikleri oluşturmaya veya yaymaya yöneltmesi şeklinde genel kast ile hareket etmesi yeterli olmaz⁸³. Bunun dışında, bu gerçeğe aykırı olduğunu bildiği içerikleri ya halk arasında endişe, korku ve panik yaratmak veya kurumları ya da şahısları hedef göstermek seçimlik amaçlarından birisi ile oluşturmaya ya da yaymaya ge-

⁸¹ Özgenç (n3) 231 vd.; Fatih Selami Mahmutoglu, Serra Karadeniz, *Türk Ceza Hukuku Genel Hükümler Şerhi*, (2. Baskı, Beta Basım, İstanbul 2021) 274 vd.; Zafer (n27) 305.

⁸² Söz konusu amaç için bakınız: Şenol (n9) 343.

⁸³ Koca, Üzülmaz (n13) 252; Şenol (n9) 343.



rekir. Örneğin, sosyal medya haberciliği yapan A'nın kullandığı X hesabından, elinde bu konuda gerçek bir bilgi olmamasına rağmen, Türkiye Cumhuriyeti vatandaşlarının kimlik verilerinin çalındığı şeklinde haber yapması söz konusu suçun manevi unsurunun oluşması için yeterli olmaz, belirtilen amaçlar ile hareket ettiğinin de ispatlanması gerekir. Yine Türkiye Cumhuriyeti vatandaşlarının verilerini ele geçirdiklerini iddia eden ve buna ilişkin bazı verileri paylaşan bilgisayar korsanlarının eylemlerine ilişkin paylaşımı yeniden paylaşım yoluyla takipçilerine duyuran bir X kullanıcısının fiili, bu fiili maddede belirtilen amaçlar ile gerçekleştirmemiş ise bu suça vücut vermez. Bunun dışında SiGüK m.16, f.5'te düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma suçu, oluşması için hem failin mutlak bilmesi hem de failin belli bir amaçla hareket etmesi arandığı için olası kastla işlenemez⁸⁴.

Bunun dışında SiGüK m.16'da düzenlenen diğer suçların manevi unsuru, kasttır. Failin kasten hareket ettiğinin kabul edilebilmesi, suçun dar anlamda tipikliğine dahil olan unsurları bilerek ve iradesini suç tipinin ihlaline yönlendirerek (isteyerek) hareket etmesine bağlıdır⁸⁵. Örneğin, failin SiGüK m.16, f.3'te düzenlenen sır saklama yükümlülüğünün ihlali suçu açısından kasten hareket etmiş olması için, açıkladığı veya gerçek ya da tüzel kişi menfaatine kullandığı bilginin, Başkanlık tarafından yürütülen görev ve faaliyetler kapsamında edinildiği, kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgiler, kişisel veriler, ticari sırlar ve bunlara ait belgelerden olduğunu bilmesi ve iradesini bunu açıklamaya veya bir gerçek ya da tüzel kişinin menfaatine kullanmaya yönlendirmesi gerekir. Yine SiGüK m.16, f.4'te düzenlenen sızıntı sonucu oluşan verileri paylaşma suçunun oluşması için, fail, paylaştığı verinin kişisel veya kritik kamu hizmeti kapsamına giren kurumsal veri olduğunu, verinin paylaşılmasında verinin sahibi olan kişi veya kurumun izninin olmadığını bilmeli ve iradesini bu veriyi paylaşmaya yöneltmelidir.

Ceza hukukunda doğrudan kastla işlenen suçların kural olarak olası kastla da işlenebileceği kabul edilir. Bunun istisnaları, suçun işlenmesi için öngörmenin yeterli olmadığı, madde metninde tam bir bilmenin arandığını gösteren ifadeler bulunan suçlar, hukuka aykırılık unsurunu tipiklik içinde düzenleyen suçlar ve isteme unsurunun oluşması için kabullenmenin yeterli olmadığı amaç saik suçlarıdır⁸⁶. Bu bakımdan SiGüK m.16'da düzenlenen suçların, 5. fıkra haricinde, olası kastla işlenmesi de mümkündür. Dolayısıyla örneğin 4. fıkra da düzenlenen sızıntı sonucu oluşan verileri erişime açma, paylaşma ve satışa çıkarma suçunu işleyen kişinin paylaştığı verinin siber uzayda veri sızıntısı nedeniyle daha önce yer alan kişisel veya kritik kamu hizmeti kapsamına giren kurumsal nitelikte bir veri ol-

⁸⁴ Artuk, Gökçen, Alşahin, Çakır (n2) 429.

⁸⁵ Özgenç (n3) 242; Hakeri (n7) 320 vd; Zafer (n27) 309.

⁸⁶ Artuk, Gökçen, Alşahin, Çakır (n2) 429.

duğunu öngörmesine rağmen bu verileri başkası ile paylaşması durumunda, söz konusu verileri bu durumu kabullenerek paylaştığı için suç olası kast ile işlenmiş olur. TCK m.61, f.2 gereğince fail hakkında cezaya hükmolunurken belirlenen temel cezanın üçte birden yarısında kadar indirilmesi gerekir (TCK m.21, f.2).

VIII. HUKUKA UYGUNLUK SEBEPLERİ

SiGüK m.16, f.2’de düzenlenen kanunen alınması gerekli onay, yetki veya iznin alınması durumunda veya f.8’de düzenlenen yasak hükümlere aykırı davranma suçunda Başkanlıktan gerekli muvafakatın veya yetkinin alınması durumunda, artık TCK m.24’te düzenlenen kanun hükmünü icra hukuka uygunluk sebebi uygulama alanı bulur, suç oluşmaz.

Meşru savunma hukuka uygunluk sebebi, SiGüK m.16’da düzenlenen suçlardan f.6’da düzenlenen siber saldırı suçunda söz konusu olabilir. Gerçekleştirilen bir siber saldırıya karşı, SGB’nin yetkilerini düzenleyen 6. maddenin 1-b fıkrası gereğince saldırıların kaynağına karşı saldırının defedilmesi için bir karşı siber saldırı düzenlenerek örneğin serverlarının devre dışı bırakılması durumunda meşru savunma ve kanun hükmünü icra hukuka uygunluk sebepleri birlikte uygulama alanı bulur.

SiGüK, m.16’da düzenlenen suçlar bir hakkın icrası kapsamında işlenebilecek nitelikte suçlar olmadığı için, TCK m.26, f.1’de düzenlenen hakkın icrası hukuka uygunluk sebebi bu suçlarda kural olarak uygulama alanı bulmaz. Hakkın icrası kapsamında ele alınması gereken tek husus, SiGüK m.16, f.5’te düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma ve yayma suçunun basının haber verme hakkı bağlamında değerlendirilmesidir⁸⁷. 5187 sayılı Basın Kanunu’nun⁸⁸ 3. maddesinde tanımlanan basının haber verme hakkı, demokratik bir toplumda bireylerin demokratik süreçlere katılırken fikir ve görüşlerini serbestçe oluşturabilmesi için vazgeçilmez nitelikte bir haktır. Bu sebeple de haber verme, bilgiyi edinme, yayma, yorumlama ve eleştirme haklarını içeren söz konusu hak, demokratik bir toplumun temel değeri olarak kabul edilir⁸⁹. Bir bilgiye ilişkin içeriğin basın özgürlüğü kapsamında değerlendirilmesi için, öncelikle bilginin Basın Kanunu m.1 gereğince söz konusu Kanun’un kapsamını oluşturan basılmış eserler veya internet haber siteleri tarafından haberleştirilmiş olması gerekir. Bu bakımdan sosyal medya haberciliği denilen kişilerin açtığı sosyal medya hesapları üzerinden haber geçerek yaptığı haberciliğin Basın Kanunu’nun kapsamında olmadığını belirtmek gerekir. İkinci olarak Yargıtay’ın aradığı, haberin en azından görünüşte gerçekliğinin olması, güncel olması, kamu yararı olması ve haberin ve-

⁸⁷ Akbulut (n2) 664; Artuk, Gökçen, Aışahin, Çakır (n2) 534 vd; Özen (n74) s.513.

⁸⁸ 26 Haziran 2004 tarihli ve 25504 sayılı Resmî Gazete’de yayımlanmıştır.

⁸⁹ AİHM Handyside v. İngiltere, 07/12/1976, par.40; AİHM Castells v. İspanya, 23.04.1992, par.43.



rilış şekli ve haberde kullanılan dilin haberin içeriği ile uyumlu olması gerekir⁹⁰. Bu açıdan en azından görünüşte doğru olduğu yönünde emareler bulunan bir veri sızıntısının haberleştirilmesi, böylesi bir haberde hem verileri sızdırılan bireylerin durumdan haberdar olması hem de kamu otoritelerinin işleyişinin denetlenmesine yönelik kamu yararı olduğu için, basının haber verme hakkı kapsamında değerlendirilmeli ve söz konusu suçu oluşturmadığı kabul edilmelidir. SiGüK m.16, f.5'te düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma ve yayma suçu, basının haber verme hakkı ile iki noktada ayrışır. İlk olarak basının haber verme hakkının kapsamında olan durumlarda, en azından görünüşte bir gerçeklik varken veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma ve yayma suçunun faili, böyle bir veri sızıntısı olmadığını bildiği halde böyle bir sızıntı varmış gibi içerik oluşturmakta veya böylesi bir içeriği yaymaktadır. Dolayısıyla kanun koyucunun basının haber verme hakkı ile bu suç tipi arasında olası bir çakışmayı önlemek için getirdiği ilk koruyucu bariyer, suç tipinde failin tam bir bilme ile hareket etmesini araması olmuştur. Bu konuda kabul edilen ikinci koruyucu bariyer ise suçun manevi unsurunun oluşması için failin halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef göstermek amacıyla hareket etmesinin aranması ile konulmuştur. Bu kriter çerçevesinde somut bir olayda yapılan bir haberin basının haber verme hakkının kapsamında mı kaldığı söz konusu suçu mu oluşturduğu değerlendirilirken, kullanılan dil ve üslup ile haberin verililiş şekli, önemli bir değerlendirme kriteri teşkil eder⁹¹.

TCK m.26, f.2'de düzenlenen ilgilinin rızası hukuka uygunluk sebebi ise mağdurunun belli bir kişi olduğu ve suç ile düzenlenen hak üzerinde mutlak suretle tasarruf etme imkanının bulunduğu suçlarda uygulama alanı bulur⁹². Bu sebeple SiGüK m.16, f.4'te düzenlenen sızıntı sonucu oluşan verilerin paylaşılması suçunun konusunun kişisel veri olduğu durumlarda, ilgilinin rızası bir hukuka uygunluk sebebi olarak tipik fiilin suç sayılmaması sonucunu doğurabilir. Ancak burada ilgilinin rızası hukuka uygunluk sebebi için aranan, rızanın fiilin icrasından önce açıklanması koşulunun gerçekleşmesi pek mümkün gözükmemektedir. Buna karşılık suçun konusunun kritik hizmetlere ilişkin veriler olması durumunda ise ilgilinin üzerinde mutlak suretle tasarrufta bulunabileceği bir hak söz konusu olmadığı için, ilgilinin rızası hukuk uygunluk sebebi uygulama alanı bulmaz. SiGüK m.16, f.4'e ilişkin zikrettiğimiz örnek dışında kalan diğer suçlarda suçun konusu mağdurunun üzerinde mutlak surette tasarrufta bulunmayacağı haklara ilişkin olduğu için ilgilinin rızası hukuka uygunluk sebebi uygulama alanı bulmaz.

⁹⁰ Akbulut (n2) 664 vd; Özen (n74) 513.

⁹¹ Akbulut (n2) 668; Özen (n74) 513.

⁹² Mahmutoğlu, Karadeniz (n80) 585 vd.

IX. TEŞEBBÜS

Teşebbüs, kasten işlenen bir suçun icra hareketlerine başlandıktan sonra maddi unsurlarının elde olmayan bir sebeple tamamlanamamasıdır. Teşebbüs manevi unsuru tamamlanmış bir suçun maddi unsurlarının tamamlanamaması halini ifade ettiği için, bazı suçların maddi yapısı itibari ile teşebbüsü elverişli olmadığı, bazı suçların ise kimi koşullara bağlı olarak teşebbüse elverişli olduğu kabul edilmektedir⁹³.

Ceza hukukunda teşebbüs hükümlerinin uygulanmasına elverişli olmadığı kabul edilen suçlardan ilki, gerçek ihmali suçlardır. Bu suçlar kural olarak bir yükümlülüğün yerine getirilmemesi ile işlenen ve tipikliğinin oluşması için bir neticenin aranmadığı suçlar olduğundan teşebbüse elverişli olmadıkları kabul edilmektedir⁹⁴. SiGüK’nde düzenlenen suçlardan, m.16, f.1’de düzenlenen istenen bilgi, belge, yazılım, veri ve donanımı vermeme veya bunların alınmasına engel olma suçu ile m.16, f.2’de düzenlenen kanunen alınması gerekli onay, yetki veya izinleri almaksızın faaliyet yürütme suçu, ilgili suçların fiil unsuruna ilişkin yapılan açıklamalarda da izah edildiği üzere gerçek ihmali suçtur. Mezkûr suçlar bu sebeple teşebbüs hükümlerinin uygulanmasına elverişli değildir. SiGüK m.16, f.9’da düzenlenen görevi ve yetkiyi kötüye kullanma suçunun her iki seçimlik hareketinin icrai veya ihmali hareket ile işlenebilmesi mümkündür. Bunlardan birinci fıkrada düzenlenen görevi ve yetkiyi kötüye kullanma fiilinin ihmali hareketle işlenmesi durumunda teşebbüs hükümlerinin uygulanması söz konusu olmaz. Fıkrada düzenlenen ikinci seçimlik hareket olan kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket etmek suretiyle veri ihlali yaşanmasına sebebiyet vermesi hareketinde ise görevin gereklerine aykırı hareketin veri ihlaline sebebiyet vermesi arandığı için neticeli bir suç söz konusudur. Bu sebeple hem görevin gereklerine aykırı hareketin icrai olarak işlendiği durumlarda bu hareketin yarıda kalması hem de veri ihlalinin gerçekleşmemesi nedeniyle neticenin meydana gelmemesi nedeniyle teşebbüs hükümleri uygulama alanı bulabilir.

SiGüK’nde düzenlenen suçlardan diğerlerinin ise sırf hareket ve soyut tehlike suçu olarak düzenlendiği görülmektedir. Sırf hareket suçlarında teşebbüs hükümlerinin uygulama alanı bulabilmesi, somut olayda failin fiili kısımlara bölerek işlemesi durumunda mümkündür⁹⁵. Örneğin, Kanun’un 6. fıkrasında düzenlenen ilk suç olan siber saldırıda bulunma suçunun kısımlara bölünerek işlenmesi pek mümkün olmadığından, teşebbüs hükümlerinin uygulanması ile de pek karşılaşılmaz. Yine aynı şekilde 2. fıkrada düzenlenen kanun uyarınca alınması gerekli onay, yetki veya izinleri almaksızın faaliyet yürütme fiilinin de kısımlara bölü-

⁹³ Koca, Üzülmöz (n13) 420; Hakeri (n7) 509.

⁹⁴ Özgenç (n3) 580.

⁹⁵ Artuk, Gökçen, Alşahin, Çakır (n2) 352.



nerek icrası mümkün olmadığından bu suç açısından da teşebbüs hükümlerinin uygulama alanı bulması mümkün gözükmemektedir. Buna karşın, 4. fıkra düzenlenenen siber uzayda veri sızıntısı nedeniyle daha önce yer alan kişisel veya kritik kamu hizmeti kapsamına giren kurumsal verileri paylaşma seçimlik hareketi, fail somut olayda paylaşma fiilini oluşturan davranışının doğrudan doğruya icrasına başlanmasına karşın onun elinde olmayan bir sebeple tamamlanamayabilir. Örneğin, veriler paylaşılacak için siber uzayda gönderilmesine rağmen teknik bir aksaklık nedeniyle paylaşılacak istenen kişi veya kişilere iletilmemiş olabilir. Bu durumda suç teşebbüs aşamasında kaldığı için, teşebbüs hükümleri uygulama alanı bulur.

X. İŞTİRAK

SiGüK m.16'da düzenlenen suçlardan, 3. fıkra düzenlenenen sır saklama yükümlülüğünün ihlali, 8. fıkra düzenlenenen yasak hükümlere aykırı davranma suçu ve 9. fıkra düzenlenenen görevi ve yetkiyi kötüye kullanma suçları özgü suç olarak düzenlendiğinden, TCK m.40, f.2 gereğince bu suçların işlenişine iştirak eden ve faillik için aranan gerekli sıfatı taşımayan kişiler, suçun işlenişine yönelik katkıları ne olursa olsun azmettiren veya yardım eden şerik olarak cezalandırılır⁹⁶. Örneğin, faillik sıfatını taşımayan bir kişi sır saklama yükümlülüğünün ihlali teşkil edecek şekilde gizlilik taşıyan bir bilgi veya kişisel veri ya da ticari sırrın açıklanması sürecinde bilgiyi internetten yayınlama gibi fiil üzerinde hakimiyet kurmuş konumda bulursa bile fail değil, yardım eden şerik olarak cezalandırılır. Yine tehdit veya cebir ile bu nitelikte bir bilginin açıklanmasını sağlayan kişi de dolaylı fail değil, ancak azmettiren şerik olarak cezalandırılabilir. Kanun'da düzenlenen ve herkes tarafından işlenebilmesi mümkün olan diğer suçlar ise iştirak kurallarının uygulanması bakımından özellik göstermez.

XI. İÇTİMA

SiGüK'nda düzenlenen suçlarda görünüşte içtima, TCK m.43, f.1'de düzenlenen zincirleme suç, TCK m.43, f.2'de düzenlenen aynı neviden fikri içtima ve TCK m.44'te düzenlenen farklı neviden fikri içtimanın uygulama alanı bulabilmesi mümkündür.

Öncelikle SiGüK m.16, f.3'te düzenlenen sır saklama yükümlülüğünün ihlali suçu ile 8. fıkrasında düzenlenen yasak hükümlere aykırı davranma suçunun ikinci seçimlik hareketi arasında, görünüşte içtima hallerinden özel - genel norm ilişkisi vardır⁹⁷. Zira SiGüK m.16, f.8'de düzenlenen suçun ikinci seçimlik hareketinin oluşması için, açıklama ve yayma fiilinin konusunu oluşturan bilgi, belge ve verilerin, SiGüK m.16, f.3'te düzenlenen ve daha özel norm niteliğinde olan sır

⁹⁶ Karakehya (n3) 241; Akbulut (n11) 938.

⁹⁷ Koca, Üzülmüş (n13) 562.

saklama yükümlülüğünün ihlali suçunun kapsamına giren, “kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgiler, kişisel veriler, ticari sırlar ve bunlara ait belgeler” den olmaması gerekir.

İkinci olarak, SiGüK m.16, f.3’te düzenlenen sır saklama yükümlülüğünün ihlali suçunun faili kural olarak TCK m.6, f.1-c gereği kamu görevlisi sıfatına sahip kişiler olacağı için, TCK m.258’de düzenlenen göreve ilişkin sırrın açıklanması suçu ile söz konu suç arasında özel - genel norm ilişkisi bulunmaktadır. Sırrın konusunun SiGüK m.13’te sayılan hususlar olması durumunda fail, sır saklama yükümlülüğünün ihlali suçundan cezalandırılır.

Üçüncü olarak, SiGüK m.4, f.1-a gereğince siber güvenlik milli güvenliğin ayrılmaz bir parçası olarak kabul edildiği için, SiGüK m.16, f.5’te düzenlenen veri sızıntısı hakkında gerçeğe aykırı içerik oluşturma veya yayma suçunun yayma seçimlik hareketi ile TCK m.217A’da düzenlenen halkı yanıltıcı bilgiyi alenen yayma suçu arasında özel - genel norm ilişkisi bulunmaktadır. Yayılan gerçeğe aykırı bilginin konusunun siber uzayda gerçekleşmiş bir veri sızıntısı olması durumunda fail, SiGüK m.16, f.5’ten dolayı cezalandırılır.

Dördüncü olarak SGB bünyesinde çalışan personelin 5237 sayılı TCK m.6, f.1-c gereğince kamu görevlisi olduğu göz önünde bulundurulduğunda, SiGüK m.16, f.9’da düzenlenen görevi ve yetkiyi kötüye kullanma suçu ile TCK m.257’de düzenlenen görevi kötüye kullanma suçu arasında, çoğu durumda özel - genel norm ilişkisi oluşur.

Beşinci olarak SiGüK m.16, f.6’da düzenlenen siber saldırı suçundan ceza verilmesi, fiilin daha ağır bir cezayı gerektiren başka bir suç oluşturmaması koşuluna bağlanmış, böylece söz konusu suç tipi ile başka suç tipleri arasında normlar çatışması olması halinde, siber saldırı suçuna ilişkin düzenlemenin cezası kendisinden daha hafif suçlar açısından asli, daha ağır suçlar açısından tali ceza normu olarak uygulama alanı bulacağı kabul edilmiştir. Bu sebeple siber saldırının bilişim sistemine girerek orada uzun süre kalma şeklinde bir gelişmiş kalıcı tehdit (APT) saldırısı olarak gerçekleştirildiği bir olayda, TCK m.243’ten, sistemin işleyişini engelleyen veya bozan bir saldırı olması durumunda TCK m.244, f.1’den, haksız kazanç elde etme amaçlı bir fidye yazılım saldırı olması durumunda TCK m.244, f.4’ten değil, cezası daha fazla olduğu için asli norm olan siber saldırı suçundan ceza verilir. Bu durumda normlar çatışması kanun koyucu tarafından görünüşte içtima kuralları ile çözüldüğü için, TCK m.44’te düzenlenen fıkri içtima kuralları ayrıca uygulama alanı bulmaz⁹⁸. Ancak örneğin bir hastanenin bilişim sistemine yapılan siber saldırı sonucunda hürriyetten yoksun kılma veya ölüm ya da yaralama neticesinin ortaya çıkması durumunda, bir suçla birden farklı suç işlendiği ve söz konusu suçların korunan hukuki değer, konu ve fiil unsuru bakımından asli - tali norm ilişkisi kurulabilecek suç tipleri

⁹⁸ Mahmutoglu, Karadeniz (n80) 1189.



olmadığı göz önüne alınarak TCK m.44'te düzenlenen farklı neviden fikri içtima kurallarına göre cezalandırma yoluna gidilmesi doğru olur.

Kanun'da düzenlenen dokuz farklı suç tipinden gerek mağduru toplum gerekse de gerçek kişi olan suçların aynı suç işleme kararının icrası kapsamında değişik zamanlarda aynı mağdura karşı birden çok kez işlenmesi halinde zincirleme suç söz konusu olur⁹⁹. Örneğin, ortak suç işleme kararı icrası kapsamında aynı kuruma ait bilişim sistemlerine değişik zamanlarda birden fazla kez siber saldırıda bulunması veya siber uzayda gerçekleşen veri sızıntısı nedeniyle elde ettiği aynı kişiye ait kişisel verilerin aynı suç işleme kararının icrası kapsamında değişik zamanlarda birden fazla kez işlenmesi halinde zincirleme suç söz konusu olur. Bu durumda fail veya failer hakkında, SiGüK m.16, f.4'te düzenlenen sızıntısı sonucu oluşan verileri paylaşma veya f.6'da düzenlenen siber saldırı suçundan bir cezaya hükmolunur, ancak verilecek ceza ¼'ten ¾'e kadar artırılır.

SiGüK'nde düzenlenen suçlardan mağduru gerçek kişi olan suçlar hakkında TCK m.43, f.2'de düzenlenen aynı neviden fikri içtima hükümleri de uygulama alanı bulabilir¹⁰⁰. Örneğin, siber saldırı sonucunda elde edilen birden fazla kişiye ait verinin birlikte satışa çıkarılması durumunda fail veya failer, SiGüK m.16, f.6'da düzenlenen siber saldırı sonucu elde edilen verinin yayılması suçunu tek fiille birden fazla kişiye karşı işlemiş olur. TCK m.43, f.2 gereğince söz konusu suç nedeniyle haklarında bir cezaya hükmolunur, ancak verilecek ceza ¼'ten ¾'e kadar artırılır.

SiGüK'nde düzenlenen suçlar hakkında TCK m.44'te düzenlenen farklı neviden fikri içtima hükümlerinin uygulama alanı bulması da mümkündür¹⁰¹. Örneğin, SiGüK m.16, f.4'te düzenlenen veri sızıntısı sonucunda oluşan verilerin erişime açılması, paylaşılması veya satışa çıkarılması suçu ile SiGüKm.16, f.6 son cümlede düzenlenen siber saldırı sonucuna elde edilen verilerin yayılması suçunun işlendiği durumlarda, suçun konusunu oluşturan verilerin konusuna göre TCK m.134'te düzenlenen özel hayatın gizliliğini ihlal, TCK m.135'te düzenlenen kişisel verilerin kaydedilmesi, TCK m.136'da düzenlenen kişisel verilerin yayılması suçları da oluşur. Yine siber uzayda elde edilen verilerin ticari sır, bankacılık veya müşteri sırrı niteliğinde olması durumunda TCK m.239'da düzenlenen suç, Devletin güvenliğine ilişkin bilgi ve belgeler olması durumunda ise TCK m.326, 329 ve 330. maddede düzenlenen suçlar da oluşur. Bu durumda fail, bir fiille işlediği birden farklı suçun cezası ağır olanından cezalandırılır. Ancak bu durum, cezanın alt sınırdan uzaklaşarak tayininde dikkate alınır¹⁰².

⁹⁹ Mahmutoglu, Karadeniz (n80) 1119; Zafer (n27) 606.

¹⁰⁰ Özgenç (n3) 693.

¹⁰¹ Akbulut (n11) 1056; Mahmutoglu, Karadeniz (n80) 1179.

¹⁰² Mahmutoglu, Karadeniz (n80) 1189.

SONUÇ

Türk hukukunda siber güvenlik alanı, 7545 sayılı Kanun ile ilk kez yasal düzenlemeye kavuşmuştur. Söz konusu alanın kanun ile düzenlenmesi, hukuk devleti adına oldukça gecikmiş bir adımdır. Söz konusu yasal düzenlemenin en olumlu yanı, içeriğinde kullanılan kavramların önemli bir kısmının yasama yorumu yöntemi ile açıklanmış olmasıdır.

Kanun'da dokuz ayrı suç tipine ve iki ayrı kabahate yer verilmiştir. Düzenlenen suç tiplerinden bir kısmı siber güvenlik alanının devlet kontrolünde faaliyet göstermesini sağlamaya, bir kısmı siber güvenlik alanının ve bu alanda yer alan verilerin korunmasına bir kısmı da siber güvenlik alanında çalışan kişilerin görevin gereklerine aykırı hareketlerinin cezalandırılmasına yöneliktir. Yapılan düzenlemeler genelde önemli sorunlar içermese de bazı noktalarda düzenleme hataları, sorunlar ve eksiklikler bulunmaktadır. Öncelikle suç tipleri düzenlenirken farklı suç tipleri olması gereken fiillerin aynı suçun seçimlik hareketi olarak veya aynı maddede düzenlendiği görülmektedir. Örneğin, SiGüK m.16, f.6'da iki ayrı cümlede düzenlenen iki ayrı suçun farklı fıkralarda düzenlenmesi, f.9'da yer verilen görev veya yetkinin kötüye kullanılması ile görevin gereklerine aykırı hareket edilerek veri ihlali yaşanmasına sebebiyet verilmesi şeklinde aynı suç tipinin alternatif seçimlik hareketleri olarak düzenlenen hallerin ayrı suç tipleri olarak düzenlenerek biri soyut tehlike diğeri zarar suçu olan bu haller için farklı cezalar öngörülmesi doğru olurdu.

İkinci olarak, 16. maddenin ile altı fıkrasında düzenlenen suç tipleri için 7. fıkra da yer verilen nitelikli haller oldukça eksiktir. Kanun'da soyut tehlike suçu olarak düzenlenen suçların somut tehlike veya zarar yol açması, neticesi sebebiyle ağırlaşmış hallerinin nitelikli hal olarak düzenlenmemiş olması, oldukça önemli bir eksiklik arz etmektedir. Yine fiilin işleniş şekli, failin amacı, suçun işlendiği zaman gibi hususlara dair nitelikli haller belirlenmemesi de önemli bir eksiklik arz etmektedir. Örneğin, siber saldırı suçunun veya sır saklama yükümlülüğünün ihlali suçunun savaş zamanı işlenmesi, siber saldırı suçunun fidye yazılım uygulaması ile gerçekleştirilmesi gibi durumların nitelikli hal olarak düzenlenmesi isabetli olurdu. Zira ülkenin elektrik alt yapısına saldırarak milyonlarca insanın hayatına ekonomik, tıbbi, sosyal açılardan zarar verilmesinin, hastanede tedavi gören çok sayıda kişinin ölümüne sebebiyet verilmesinin üst sınırı on altı yıl hapis cezası gerektiren bir suç olarak düzenlenmesi kanaatimizce oldukça isabetsizdir.

Üçüncü olarak çalışmanın içtima başlığı altında ayrıntılı olarak açıklanmaya çalışıldığı üzere Kanun'da yer alan suçlar ile TCK'da düzenlenen çeşitli suçlar arasında hem özel norm genel norm ilişkisi hem de çoğu durumda fikri içtima ilişkisi ortaya çıkacaktır. Bu sebeple TCK m.243 ve m.244'te düzenlenen bilişim suçları ile siber güvenlik alanındaki suçların birlikte mütalaa edilmesi, bilişim suçlarının çoğu durumda başka suçların işlenmesinde araç olarak kullanıldığı göz önüne alındığında, TCK m.212'dekine benzer bir düzenleme ile TCK m.44'te



düzenlenen farklı neviden fikri içtima düzenlemesinin bu suçlarda uygulanmasının sağlanması isabetli olurdu. Zira mevcut durumda, örneğin bir elektrik veya ulaşım şebekesine yapılan siber saldırı sonucu çok sayıda kişinin uzun süreli hürriyetinden yoksun kılınması hatta yaralanma veya ölümüne neden olunması durumunda TCK m.44 gereğince işlenen çok ciddi suçlardan bir kısmının ceza verilememesi durumu ile karşılaşılacaktır.

Bunların dışında siber güvenlik milli güvenliği ayrılmaz bir parçası olarak tanımlandığı için devletin güvenliğine ilişkin suçlar ile bu suçların birlikte ele alınması, sınırlarının belirgin bir biçimde belirlenmesi de daha doğru olurdu. Zira mevcut durumda, Türk hukukunda konuya ilişkin kavramların yeterince net olmaması nedeniyle geniş bir yorumla siber güvenliğe ilişkin suçların oluştuğu çoğu durumda aynı zamanda devletin güvenliğine yönelik suçların da oluştuğu ileri sürülebilecektir.

KAYNAKÇA

Akbulut B, Ceza Hukuku Genel Hükümler, (9. Baskı, Adalet Yayınevi, Ankara 2022)

Akbulut B, Bilişim Suçları, (2. Baskı, Adalet Yayınevi, Ankara 2017)

Artuk M E, Gökçen A, Alşahin M E, Çakır K, Ceza Hukuku Genel Hükümler, (16. Baskı, Adalet Yayınevi, Ankara 2022)

Artuk M E, Gökçen A, Alşahin M E, Çakır K, Ceza Hukuku Özel Hükümler, (20. Baskı, Adalet Yayınevi, Ankara 2022)

Bayraktar K, Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar, Özel Ceza Hukuku (C.III, On İki Levha Yayıncılık, İstanbul 2018)

Değirmenci O, Ceza Muhakemesinde Sayısal (Dijital) Delil, (Seçkin Yayıncılık, Ankara 2014)

Hakeri, H, Ceza Hukuku Genel Hükümler, (23. Baskı, Adalet Yayınevi, Ankara, 2020)

Kaplan M, “Türk Ceza Hukukunda Kamu Görevlisi Kavramı”, (Aralık 2015) 5(2), Akdeniz Üniversitesi Hukuk Fakültesi Dergisi 49-77.

Karakehya H, Ceza Hukuku Genel Hükümler, (Adalet Yayınevi, Ankara 2022).

Koca M, Üzülmöz İ, Türk Ceza Hukuku Genel Hükümler, (15. Baskı, Seçkin Yayıncılık, Ankara 2022).

Koca M, Üzülmöz İ, Türk Ceza Hukuku Özel Hükümler, (8. Baskı, Adalet Yayınevi, Ankara 2022).



Mahmutoğlu F S, Karadeniz S, Türk Ceza Hukuku Genel Hükümler Şerhi, (2. Baskı, Beta Basım, İstanbul 2021).

Okuyucu Ergün, G, “Görevi Kötüye Kullanma Suçu”, (2009), (82), TBB Dergisi 1-31.

Özbek V Ö, Doğan K, Bacaksız P, Ceza Hukuku Genel Hükümler, (15. Baskı, Seçkin Yayıncılık, Ankara 2024).

Özbek V Ö, Doğan K, Bacaksız P, Ceza Hukuku Özel Hükümler, (19. Baskı, Seçkin Yayıncılık, Ankara 2024).

Özen M, Atacan K, Göreve İlişkin Sırrın Açıklanması Suçu”, (2020), 69(1), Ankara Üniversitesi Hukuk Fakültesi Dergisi, 189-232.

Özen, M, Ceza Hukuku Özel Hükümler, (9. Baskı, Adalet Yayınevi, Ankara 2024).

Özgenç İ, Türk Ceza Hukuku Genel Hükümler, (18. Baskı, Seçkin Yayıncılık, Ankara 2022).

Sevük H Y, “Görevi Kötüye Kullanma Suçu (TCK m.257)”, (2018), 23(39), DÜHFD, 257-316.

Şenol C, “Halkı Yanıltıcı Bilgiyi Alenen Yayma Suçu”, (Aralık 2022), 17(20), Ceza Hukuku Dergisi 331-352.

Tezcan D, Erdem, M R, Önok R M, Teorik ve Pratik Ceza Özel Hukuku, (20. Baskı, Seçkin Yayıncılık, Ankara 2022).

Turgut B, “Türk Ceza Hukukunda Verileri Yok Etmeme Suçu (TCK m.138)”, (Mart 2025) (233) Terazi Hukuk Dergisi 129-139.

Turgut B, “Siber Uzayda Yer Alan Kişisel veya Kritik Kamu Hizmeti Kapsamına Giren Kurumsal Verileri Erişime Açma, Paylaşma ve Satışa Çıkarma Suçu”, (Haziran 2025) (16) İnönü Üniversitesi Hukuk Fakültesi Dergisi, 207-220.

Usta O, Kişilik Hakkı Bağlamında Unutulma Hakkı, (Adalet Yayınevi, Ankara 2023).

Yamaner Özdemir M, Uyuşturucu veya Uyarıcı Madde İmal ve Ticareti Suçu (TCK m.188) (Seçkin Yayıncılık, Ankara 2022).

Yıldırım Yeniman E, “Bilişim Sistemlerine Yönelik Siber Saldırıları ve Siber Güvenliğin Sağlanması”, (2018) 7(2) Mesleki Bilimler Dergisi 24-33.

Zafer H, Ceza Hukuku Genel Hükümler, (8. Bası, Beta Yayım, İstanbul 2021)

