

Bilgi, Belge, Yazılım, Veri ve Donanım Vermeme veya Engel Olma Suçu

Av. Burak Üçüncü · 3 Mayıs 2026 · 7 dk okumaGüncelleme: 5 Mayıs 2026

Siber Güvenlik Kanunu, Türkiye'nin siber güvenlik mimarisini yeniden şekillendiren ve bu alanda ilk kez kapsamlı bir yasal çerçeve sunan düzenleme olarak 19 Mart 2025 tarihinde yürürlüğe girmiştir. Kanun'un beşinci bölümünde yer alan cezai hükümler arasında, 16. maddenin birinci fıkrası, [Siber Güvenlik Başkanlığı](#)'nın denetim ve gözetim fonksiyonlarının etkinliğini güvence altına almaya yönelik özel bir suç tipi düzenlemektedir.

[Siber Güvenlik Kanununda düzenlenen suçlardan](#) ilki olan bu suç tipinin kanun metnindeki karşılığı şöyledir:

Siber Güvenlik Kanunu m.16/1

"Kamu kurum ve kuruluşları hariç olmak üzere bu Kanunla yetkilendirilen mercilerin ve denetim görevlilerinin görev ve yetkileri kapsamında istedikleri bilgi, belge, yazılım, veri ve donanımı vermeyenler veya bunların alınmasına engel olanlar bir yıldan üç yıla kadar hapis ve beşyüz günden binbeşyüz güne kadar adli para cezası ile cezalandırılır."

Kanun koyucu bu düzenlemeyle, Siber Güvenlik Başkanlığı'nın görev ve yetkilerini fiilen kullanabilmesini ceza hukuku yaptırımıyla teminat altına almayı amaçlamıştır. Zira siber güvenlik alanında etkin bir denetim mekanizması kurulabilmesi, denetlenen kişi ve kuruluşların işbirliği yapmasına doğrudan bağlıdır. Bu işbirliğinin sağlanamaması halinde, Kanun'un öngördüğü koruma sisteminin bütünüyle işlevsiz kalması söz konusu olabilecektir.

BÖLÜM I

Korunan Hukuki Değer

Suçla korunan hukuki değer, öncelikli olarak Siber Güvenlik Başkanlığı'nın denetim ve gözetim faaliyetlerinin işleyişidir. Daha geniş bir perspektiften bakıldığında ise korunan değer, Kanun'un bütüncül amacı olan ulusal siber güvenliğin sağlanması olduğu söylenebilir.

Siber Güvenlik Başkanlığı, Kanun'un 5. ve 6. maddeleri uyarınca kritik altyapıların korunması, siber saldırıların tespiti, siber tehdit istihbaratı elde edilmesi, zafiyet ve sızma testlerinin yürütülmesi gibi hayati görevler üstlenmektedir. Bu görevlerin yerine getirilmesi, kaçınılmaz olarak ilgili kuruluşlardan bilgi, belge, yazılım, veri ve donanım temin edilmesini gerektirmektedir. Dolayısıyla bu suç tipi, Başkanlığın operasyonel kapasitesini doğrudan koruma altına almaktadır.

Bu bağlamda suç, kamu idaresinin işleyişine karşı suçlarla benzer bir koruma fonksiyonu üstlenmekle birlikte, siber güvenlik alanına özgü niteliği itibarıyla kendine has bir kategori oluşturmaktadır.

BÖLÜM II —

Suçun Maddi Unsurları

A. Fail

Suçun faili, kamu kurum ve kuruluşları dışında kalan gerçek ve tüzel kişilerdir. Kanun koyucu, kamu kurum ve kuruluşlarını açık bir hükümle suçun kapsamı dışında bırakmıştır. Bu tercih, kamu kurumlarının Başkanlıkla olan ilişkisinin idari hiyerarşi ve koordinasyon mekanizmaları çerçevesinde çözümlenmesinin daha uygun görülmesinden kaynaklanmaktadır.

Fail olabilecek kişiler arasında özel sektör kuruluşları, siber güvenlik şirketleri, internet servis sağlayıcıları, elektronik haberleşme işletmecileri, veri merkezi işletmecileri ve siber uzayda faaliyet yürüten diğer tüm gerçek ve tüzel kişiler sayılabilir. Tüzel kişiler bakımından ise cezai sorumluluk, TCK'nın genel hükümleri çerçevesinde, fiili gerçekleştiren gerçek kişi üzerinden değerlendirilecektir.

Suç, özgü suç niteliği taşımamaktadır. Başkanlık tarafından bilgi veya belge talep edilen herkes potansiyel fail sıfatına sahiptir. Ancak talebin muhatabı olmayan bir kişinin bu suçu işlemesi mümkün değildir; zira suçun oluşması için öncelikle yetkili merciler tarafından usulüne uygun bir talebin yöneltmiş olması gerekmektedir.

B. Mağdur

Suçun mağduru, doğrudan Siber Güvenlik Başkanlığı ve dolaylı olarak kamudur. Başkanlığın denetim fonksiyonunun engellenmesi, nihai tahlilde toplumun siber güvenlik hakkının ihlal edilmesi anlamına gelmektedir.

C. Fiil

Suçun maddi unsurunu oluşturan fiil, iki seçimlik hareketle gerçekleştirilebilir:

Birinci seçimlik hareket, Kanunla yetkilendirilen mercilerin ve denetim görevlilerinin görev ve yetkileri kapsamında istedikleri bilgi, belge, yazılım, veri ve donanımı *vermemektir*. Bu, ihmali bir davranışla gerçekleştirilen bir suç tipidir. Talebin muhatabı, istenen şeyleri süresi içinde teslim etmemek suretiyle suçu işlemiş olur.

Bu noktada dikkat edilmesi gereken husus, talebin kapsamıdır. Kanun, talep konusu materyalleri oldukça geniş bir şekilde belirlemiştir: bilgi, belge, yazılım, veri ve donanım. Yazılım ve donanımın da talep kapsamına alınmış olması, bu suç tipini klasik bilgi ve belge vermeme suçlarından ayıran önemli bir özelliktir. Örneğin, Başkanlığın bir zafiyet testi kapsamında belirli bir yazılımın kaynak kodunu veya bir donanım bileşenini fiziken teslim edilmesini talep etmesi durumunda, bu talebin yerine getirilmemesi suçun oluşmasına yol açabilecektir.

İkinci seçimlik hareket ise talep edilen bilgi, belge, yazılım, veri ve donanımın *alınmasına engel olmaktır*. Bu, icrai bir davranışla gerçekleştirilen bir suçtur. Fail, denetim görevlilerinin ilgili materyallere erişimini aktif olarak engellemekte, örneğin verileri silmekte, sistemlere erişimi kısıtlamakta veya fiziksel olarak denetim

ekibinin çalışmasını önlemektedir. Bu seçimlik hareket, salt pasif direniş olan birinci seçimlik harekete kıyasla daha ağır bir haksızlık içeriğine sahip olmakla birlikte, kanun koyucu her iki hareket için aynı ceza çerçevesini benimsemiştir.

D. Talebin Niteliği

Suçun oluşabilmesi için talebin, Kanunla yetkilendirilen merciler veya denetim görevlileri tarafından, görev ve yetkileri kapsamında yapılmış olması zorunludur. Görev kapsamı dışında kalan veya yetkisiz kişilerce yapılan talepler, bu suçun oluşmasına elverişli değildir. Bu durum, suçun bir ön koşulunu oluşturmaktadır.

Kanun'un 6. maddesinin birinci fıkrasının (ç) bendi, Başkanlığın yürüttüğü faaliyetlerle sınırlı olmak üzere bilgi, belge, veri ve kayıtları alabileceğini düzenlemektedir. Aynı bentte, talepte bulunulanların kendi mevzuatlarındaki hükümleri gerekçe göstererek talebi reddedemeyecekleri de açıkça ifade edilmiştir. Bu hüküm, örneğin bankacılık sırrı, ticari sır veya kişisel verilerin korunması gibi gerekçelerin, Başkanlığın talebi karşısında ileri sürülemeyeceğini ortaya koymaktadır.

Kanun'un 8. maddesinin dördüncü fıkrası ise denetimle görevlendirilenlerin yetkilerini somutlaştırmaktadır. Buna göre denetim görevlileri; elektronik ortamdaki verilerin, belgelerin, elektronik altyapının, cihaz, sistem, yazılım ve donanımlarının incelenmesi, bunlardan kopya, dijital suret veya örnek alınması ve yazılı veya sözlü açıklama istenmesi konularında yetkilidir.

BÖLÜM III

Suçun Manevi Unsuru

Kanun'da özel bir kast türü aranmamıştır. Dolayısıyla suçun manevi unsuru, genel kasttır. Failin, Kanunla yetkilendirilen mercilerin talebini bilmesi ve buna rağmen istenen materyali vermemesi ya da alınmasını engellemesi yeterlidir.

Taksirle işleme hali düzenlenmediğinden, failin talebi bilmemesi veya teknik nedenlerle yerine getirememesi gibi durumlarda kastın varlığından söz edilemeyecektir. Örneğin, talebin ilgili kişiye usulüne uygun şekilde tebliğ edilmemiş olması veya talep edilen verinin teknik olarak mevcut olmaması hallerinde, suçun manevi unsuru gerçekleşmemiş olacaktır.

BÖLÜM IV

Yaptırım

Suç için öngörülen yaptırım, bir yıldan üç yıla kadar hapis cezası ve beş yüz günden bin beş yüz güne kadar adli para cezasıdır. Her iki cezanın birlikte (kümülatif olarak) uygulanacağı hususu, madde metninden açıkça anlaşılmaktadır.

Hapis cezasının alt sınırının bir yıl olarak belirlenmesi, hükmün açıklanmasının geri bırakılması (HAGB) ve kısa süreli hapis cezasının seçenek yaptırımlara çevrilmesi gibi müesseselerin uygulanabilmesine olanak tanımaktadır. Bu durum, suçun ilk kez işlendiği ve somut olayın koşullarının elverişli olduğu hallerde, failin cezaevine girmeksizin yaptırımla karşılaşmasını mümkün kılmaktadır.

Adli para cezasının gün birimli olarak düzenlenmiş olması, TCK'nın 52. maddesi uyarınca günlük miktarın yirmi Türk lirasından beş yüz Türk lirasına kadar belirlenmesine olanak tanımaktadır. Dolayısıyla adli para

cezası, somut olayda on bin TL ile yedi yüz elli bin TL arasında bir aralıkta belirlenecektir.

BÖLÜM VI

Nitelikli Haller

Kanun'un 16. maddesinin yedinci fıkrası uyarınca, bu suç bakımından da ağırlaştırıcı sebepler uygulanacaktır:

Suçun kamu görevlisi tarafından işlenmesi halinde ceza üçte bir oranında artırılabilecektir. Her ne kadar birinci fıkra da kamu kurum ve kuruluşları fail kapsamı dışında tutulmuş olsa da, kamu görevlisi sıfatını taşıyan bir gerçek kişinin özel sektördeki faaliyetleri çerçevesinde bu suçu işlemesi teorik olarak mümkündür.

Suçun birden fazla kişi tarafından birlikte işlenmesi halinde ceza yarı oranında artırılabilecektir. Örneğin, bir şirketin yönetim kurulu üyelerinin ortak kararla denetim talebini reddetmesi bu kapsamda değerlendirilebilir.

Suçun bir örgütün faaliyeti çerçevesinde işlenmesi halinde ceza yarısından iki katına kadar artırılabilecektir.

BÖLÜM VII

Diğer Suç Tipleriyle İlişkisi

Bu suç tipinin, TCK'daki bazı düzenlemelerle ilişkisi üzerinde durulması gerekmektedir.

TCK'nın 265. maddesinde düzenlenen *görevi yaptırmamak için direnme* suçu ile 16/1'deki suç arasında fikri içtima gündeme gelebilir. Denetim görevlilerine fiziksel olarak engel olunması halinde her iki suç tipinin unsurları da gerçekleşebilmektedir. Bu durumda, TCK'nın 44. maddesi uyarınca en ağır cezayı gerektiren suçtan ceza verilmesi gerekecektir.

Ayrıca, TCK'nın 243. maddesinde düzenlenen *bilişim sistemine girme* suçu ile de dolaylı bir ilişki söz konusu olabilir. Denetim görevlilerinin erişimini engellemek amacıyla sistemlerin kapatılması veya verilerin silinmesi, aynı zamanda TCK'nın 244. maddesindeki *sistemi engelleme, bozma, verileri yok etme veya değiştirme* suçunu da oluşturabilir.

BÖLÜM VIII

Uygulamada Karşılaşılabilecek Sorunlar

Bu suç tipinin uygulamasında bazı sorunlu noktaların ortaya çıkması muhtemeldir.

Başkanlığın talep edebileceği materyallerin sınırları, özellikle "yazılım" ve "donanım" kavramları bakımından tartışmalı olabilir. Bir şirketin ticari yazılımının kaynak kodunun veya özel mülkiyet niteliğindeki donanımın tesliminin talep edilmesi, orantılılık ilkesi bakımından soru işaretleri doğurabilir.

Kanun, talebin yerine getirilmesi için belirli bir süre öngörmemektedir. Talebin "gecikmeksizin" mi yoksa "makul sürede" mi yerine getirilmesi gerektiği, uygulamada netleştirilmeye muhtaçtır.

Talep edilen verinin teknik olarak mevcut olmaması veya erişimin mümkün olmaması halinde, failin cezai sorumluluğunun bulunmayacağı açıktır. Ancak bu durumun ispat yükünün kime ait olacağı tartışmalıdır.

Kanun'un 6. maddesinin birinci fıkrasının (ç) bendindeki "kendi mevzuatındaki hükümleri gerekçe göstererek kaçınmaz" hükmü, KVKK ve ticari sır koruması bakımından önemli bir istisna oluşturmaktadır. Bu hükmün

Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunması hakkı ile ilişkisi ayrıca değerlendirilmelidir.

BÖLÜM IX —

Sonuç

7545 sayılı Siber Güvenlik Kanunu'nun 16. maddesinin birinci fıkrasında düzenlenen bilgi, belge, yazılım, veri ve donanım vermeme veya engel olma suçu, Kanun'un öngördüğü denetim mekanizmasının etkinliğini güvence altına alan temel bir düzenlemedir. Suçun hem ihmali hem de icrai davranışla işlenebilmesi, talebin kapsamının son derece geniş tutulması ve kümülatif yaptırım öngörülmesi, kanun koyucunun bu konudaki kararlılığını açıkça ortaya koymaktadır.

Bununla birlikte, talebin kapsamı, süre, orantılılık ve temel haklar bakımından ortaya çıkabilecek sorunların, ikincil mevzuat ve içtihatlarla netleştirilmesi büyük önem taşımaktadır. Özellikle Kanun'un Geçici 1. maddesi uyarınca bir yıl içinde çıkarılması öngörülen uygulama düzenlemelerinin, bu boşlukları gidermesi beklenmektedir.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/bilgi-belge-yazilim-veri-ve-donanim-vermeme-veya-engel-olma-sucu>