

Siber Güvenlik Kanunundaki Suçlar

19 Mart 2025 tarihinde Resmi Gazete’de yayımlanarak yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, Türk hukuk sistemine köklü yenilikler getirmiştir.

Av. Burak Üçüncü · 26 Mart 2026 · 4 dk okumaGüncelleme: 6 Ekim 2026

19 Mart 2025 tarihinde Resmi Gazete’de yayımlanarak yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, Türk hukuk sistemine köklü yenilikler getirmiştir. Kanun, Türkiye’nin siber uzaydaki milli gücünü koruma altına alma hedefiyle hazırlanmış olup, siber güvenliği milli güvenliğin ayrılmaz bir parçası olarak tanımlamaktadır.

Kanun’un en dikkat çekici yönlerinden biri, 16. maddesinde düzenlenen ceza hükümleridir. Bu maddede dokuz ayrı suç tipi öngörülmüş; adli para cezasından on beş yıla kadar hapis cezasına uzanan geniş bir yaptırım yelpazesi oluşturulmuştur. Söz konusu suç tipleri, yalnızca siber saldırganları değil, bilgi verme yükümlülüğünü ihlal eden gerçek ve tüzel kişileri, sır saklama yükümlülüğünü yerine getirmeyen kamu görevlilerini ve hatta asılsız veri sızıntısı iddiası yayan kişileri de hedef almaktadır.

Bu yazı dizisinde, Siber Güvenlik Kanununun 16. maddesinde yer alan her bir suç tipini ayrı ayrı inceleyeceğiz. Her yazıda ilgili suçun maddi ve manevi unsurları, faillik durumu, yaptırımları, nitelikli halleri ve uygulamada karşılaşılabilecek sorunlar ele alınacaktır.

1. Bilgi, Belge, Yazılım, Veri ve Donanım Vermeme veya Engel Olma Suçu (m.16/1)

Siber Güvenlik Başkanlığı’nın ve denetim görevlilerinin görev ve yetkileri kapsamında talep ettikleri bilgi, belge, yazılım, veri ve donanımı vermeyenler veya bunların alınmasına engel olanlar hakkında öngörülen suç tipidir. Kamu kurum ve kuruluşları bu suçun kapsamı dışında tutulmuş olup, yaptırım olarak bir yıldan üç yıla kadar hapis ve beş yüz günden bin beş yüz güne kadar adli para cezası öngörülmüştür.

2. İzinsiz Faaliyet Yürütme Suçu (m.16/2)

Kanun uyarınca alınması gereken onay, yetki veya izinleri almaksızın siber güvenlik alanında faaliyet yürütenlere yönelik düzenlemedir. İki yıldan dört yıla kadar hapis ve bin günden iki bin güne kadar adli para cezası öngörülmüştür. Bu suç tipi özellikle siber güvenlik sektöründe faaliyet gösteren şirketler, dernekler ve vakıflar bakımından büyük önem taşımaktadır.

3. Sır Saklama Yükümlülüğünü İhlal Suçu (m.16/3)

Kanun’un 13. maddesinde düzenlenen sır saklama yükümlülüğüne aykırı davranışlar hakkında dört yıldan sekiz yıla kadar hapis cezası öngörülmüştür. Başkanlık bünyesinde edinilen gizli bilgilerin, kişisel verilerin ve ticari sırların yetkisiz kişilerle paylaşılması bu suç kapsamında değerlendirilmektedir.

4. Kişisel veya Kurumsal Verileri İzinsiz Erişime Açma, Paylaşma veya Satışa Çıkarma Suçu (m.16/4)

Siber uzayda veri sızıntısı sonucu ortaya çıkan kişisel veya kritik kamu hizmeti kapsamına giren kurumsal verileri, ilgili kişilerin veya kurumların izni olmaksızın erişime açan, paylaşan ya da satışa çıkaranlara üç yıldan beş yıla kadar hapis cezası öngörülmüştür. Bu suç tipi, özellikle veri sızıntılarının ardından "leak" forumlarında ve karanlık ağda (dark web) faaliyet gösterenler açısından doğrudan uygulanabilir niteliktedir.

5. Asılsız Veri Sızıntısı İddiası Suçu (m.16/5)

Siber uzayda veri sızıntısı olmadığını bildiği halde, halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef göstermek amacıyla gerçeğe aykırı içerik oluşturan veya yayanlara iki yıldan beş yıla kadar hapis cezası öngörülmüştür. Bu düzenleme, özellikle sosyal medya üzerinden yayılan asılsız siber saldırı ve veri sızıntısı haberlerine karşı caydırıcı bir işlev üstlenmektedir.

6. Milli Güce Yönelik Siber Saldırı Suçu (m.16/6)

Kanun'un en ağır yaptırımını içeren suç tipidir. Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren unsurlara yönelik siber saldırıda bulunanlara sekiz yıldan on iki yıla kadar hapis cezası; bu saldırı sonucu elde edilen verileri yayan, gönderen veya satışa çıkaranlara ise on yıldan on beş yıla kadar hapis cezası öngörülmüştür. Tali norm niteliğinde düzenlenmiş olup, fiil daha ağır cezayı gerektiren başka bir suç oluşturduğu takdirde o suçtan ceza verilecektir.

7. Yasak Hükümlerine Aykırılık Suçu (m.16/8)

Kanun'un 12. maddesinde düzenlenen yasak hükümlerine aykırı davranan eski Başkanlık personeline üç yıldan beş yıla kadar hapis cezası öngörülmüştür. Bu yasak; görevden ayrıldıktan sonra iki yıl süreyle siber güvenlik alanında başka görev almayı, ticaret yapmayı ve Başkanlık faaliyetleri kapsamında edinilen bilgileri yayımlamayı kapsamaktadır.

8. Görevi Kötüye Kullanma ve Veri İhlaline Sebebiyet Verme Suçu (m.16/9)

Kanun'dan kaynaklanan görev ve yetkilerini kötüye kullanan veya kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket ederek veri ihlali yaşanmasına sebebiyet verenlere bir yıldan üç yıla kadar hapis cezası öngörülmüştür. Bu suç tipi, TCK'daki genel görevi kötüye kullanma suçuna göre özel norm niteliği taşımaktadır.

9. Nitelikli Haller (m.16/7)

Yukarıdaki suçların tamamı bakımından geçerli olan ağırlaştırıcı sebeplerdir. Suçun kamu görevlisi tarafından işlenmesi halinde ceza üçte bir oranında, birden fazla kişi tarafından birlikte işlenmesi halinde yarı oranında, bir örgütün faaliyeti çerçevesinde işlenmesi halinde ise yarısından iki katına kadar artırılmaktadır.

Kanun, ceza hükümlerinin yanı sıra ciddi tutarlarda idari para cezaları da öngörmektedir. Siber güvenliğe ilişkin tedbir alma ve bildirim yükümlülüklerini yerine getirmeyenlere bir milyon TL'den on milyon TL'ye kadar; siber güvenlik ürünlerinin ihracatına ilişkin yükümlülükleri yerine getirmeyenlere ise on milyon TL'den yüz milyon TL'ye kadar idari para cezası uygulanabilecektir. Ticari şirketler bakımından bu ceza, brüt satış hasılatının yüzde beşine kadar çıkabilmektedir.

7545 sayılı Kanun'un ceza hükümleri incelendiğinde, kanun koyucunun siber güvenlik alanında son derece caydırıcı bir yaptırım rejimi oluşturma iradesinde olduğu açıkça görülmektedir. Özellikle milli güce yönelik siber saldırı suçunda on beş yıla kadar çıkabilen hapis cezası, bu iradenin en somut yansımasıdır. Bununla birlikte, Kanun'un bazı hükümleri uygulamada tartışmalara yol açabilecek niteliktedir. Örneğin, milli gücü meydana getiren unsurlar kavramının sınırlarının belirsizliği, asılsız veri sızıntısı iddiası suçundaki bildiği halde unsurunun ispatı ve izinsiz faaliyet yürütme suçunun kapsamı gibi konular, doktrinde ve içtihatlarda netleştirilmeye muhtaçtır. Ayrıca, Kanun'un TCK'daki mevcut bilişim suçları (m.243-246) ile ilişkisi de ayrıca değerlendirilmelidir. Özellikle milli güce yönelik siber saldırı suçundaki tali norm kaydı, bu ilişkinin düzenlenmesi bakımından önemli bir başlangıç noktası sunmaktadır; ancak diğer suç tipleri bakımından içtima sorunlarının gündeme gelmesi muhtemeldir.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/siber-guvenlik-kanunundaki-suclar>