

T.C.
BİLGİ ÜNİVERSİTESİ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS DERSİ ÖDEVİ

SİBER GÜVENLİK KANUNU KAPSAMINDA YER ALAN SUÇ VE KABAHLER
İLE SİBER GÜVENLİK DENETİMİ SIRASINDA İŞ BİRLİĞİNDE BULUNMAMA
SUÇU

Hazırlayan: Şeymanur Sağınç
Öğrenci No:125691018

1. Siber Güvenlik Kanunu ve Düzenlenen Suç ve Kabahatler

7545 sayılı Siber Güvenlik Kanunu (“Kanun”) 19.03.2025 tarihinde Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Kanun, Türkiye'nin siber uzaydaki güvenliğini tehdit eden iç ve dış tehditleri tespit edip bertaraf etmek, kamu ve özel kuruluşları siber saldırılara karşı korumak, ulusal siber güvenlik strateji ve politikalarını belirlemek ve Siber Güvenlik Kurulu'nu (“Kurul”) kurmak amacıyla çıkarılmıştır.

Kanun’un “Cezai Hükümler ve İdari Para Cezalarının Uygulanması” başlıklı beşinci bölümünün 16. maddesinde cezai hükümler ve idari para cezaları düzenlenmiş olup, söz konusu maddede;

- Siber güvenlik denetimi sırasında iş birliğinde bulunmama suçu,
- İzinsiz siber güvenlik faaliyetinde bulunma suçu,
- Sır ifşası suçu,
- Kişisel ve kurumsal verileri ifşa suçu,
- Veri sızıntısı söylentisi çıkarma suçu,
- Milli unsurlara yönelik siber saldırı suçu,
- Milli unsurlara ait verileri ifşa suçu,
- Siber Güvenlik Başkanlığı (“Başkanlık”) personeline getirilen yasaklamalara aykırı davranılması suçu ve
- Veri ihlaline sebebiyet verme suçu

olmak üzere 9 farklı suç¹,

- “Sorumluluk ve iş birliği” başlıklı 7. maddenin b ve c bentleri kapsamında zafiyet ve siber olayları Başkanlığa bildirmeyen veya yetkisiz kaynaklardan siber güvenlik ürünü tedarik etmek,
- “Denetim” başlıklı 8. maddenin 4. fıkrası kapsamında denetçilerin inceleme yapabilmesi için gerekli cihaz, sistem ve alt yapıyı hazır bulundurmamak ve

¹ Kaya, Mehmet Bedii; *Siber Güvenlik Hukuku*, s. 321.

- “Siber güvenlik ürünleri ve şirketleri” başlıklı 18. madde kapsamında siber güvenlik şirketlerinin yurt dışı satış, birleşme veya pay devri gibi işlemlerini Başkanlığa bildirmeden ya da onay almadan gerçekleştirmesi

olmak üzere 3 farklı kabahat ihdas edilmiştir.

2. Siber Güvenlik Denetimi Sırasında İş Birliğinde Bulunmama Suçu

İşbu ödev kapsamında söz konusu suç ve kabahatler arasında 16. maddenin 1. fıkrasında düzenlenen “Siber güvenlik denetimi sırasında birliğinde bulunmama suçu” incelenmiş olup; söz konusu madde aşağıdaki şekildedir:

“Cezai hükümler ve idari para cezaları

MADDE 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.”*

2.1. Suçun Maddi Unsurları:

- a. **Fiiil:** Madde özü itibariyle siber güvenlik denetimi sırasında bilgi, belge, donanım vermeyenler veya engel olanlar için bir düzenleme barındırmakta olup, söz konusu düzenleme uyarınca suç teşkil edecek fiil; bilgi, belge, yazılım, veri veya donanım vermemek veya bunların alınmasına engel olmak olarak nitelendirilebilir.
- b. **Fail:** Kamu kurum ve kuruluşları hariç olmak üzere; gerçek kişiler, özel hukuk tüzel kişileri ve tüzel kişiliği bulunmayan kuruluşlar fail olabilir.
- c. **Suçtan Zarar Gören:** Maddenin amacı itibariyle tüm toplumun mağdur sayılabileceği söylenebilir².

² Şenol, Cem; "7545 Sayılı Siber Güvenlik Kanunu'nda Düzenlenen Suçlar", *Türkiye Adalet Akademisi Dergisi*, Yıl 16, Sayı 63, Temmuz 2025, s. 173.

- d. Konu:** Yetkili merciin görev ve yetkileri kapsamında talep ettiği bilgi, belge, yazılım, veri ve donanımdır. Bu kapsamda suçun konusu; istenen bilgi, belge, yazılım, veri veya donanımın verilmemesi veya engel olunması hâlini kapsar.
- e. Nitelikli Hâl:** Madde kapsamında suça ilişkin yaptırım 1 yıldan 3 yıla kadar ve 500 günden 1500 güne kadar adli para cezası belirlenmiş olup, suçun Kanun'un 16. maddesinin 7. fıkrası uyarınca suçun; kamu görevlisi tarafından işlenmesi halinde üçte bir oranında, birden fazla kişi tarafından işlenmesi halinde yarı oranında ve bir örgütün faaliyeti çerçevesinde işlenmesi halinde yarısından katına kadar artırımı uygulanacağı düzenlenmiştir.

2.2. Suçun Manevi Unsurları:

Söz konusu maddede suçun taksirle işlenebileceği düzenlenmediği için suç ancak kast ile işlenebilecek bir suçtur. İstenen bilgi, belge, yazılım, veri veya donanımın verilmemesi veya engel olunması hâlinde suç oluşur, ayrıca bir neticenin oluşması aranmaz.

3. Suçun Bilişim Hukuku Perspektifinden Değerlendirilmesi

3.1. Talep edilen bilgi, belge, yazılım, veri ve donanımın sınırı

Madde, doğrudan yetkili merci ve denetim görevlilerinin görev ve yetkileri kapsamında istenilen bilgi, belge, yazılım, veri ve donanımın verilmemesi veya verilmesine engel olunması suçunu düzenlemekte olup, talep edilecek veya verilmesi engellenen bilgi, belge, yazılım, veri ve donanımın hangi sınırlar içinde talep edilebileceği detaylandırılmamış olup, bu itibarla maddenin sınırları belirsizlik yaratmaktadır.

Talebin kapsamı bakımından:

Bilgi: Talep edilen bilginin ticari sır ihtiva etmesi ve avukat-müvekkil gizliliğinin korunması gereken hâller bakımından risk teşkil edebilecek niteliktedir.³

Belge: Talep edilen belgenin/belgelerin ticari sır ihtiva etmesi ve avukat-müvekkil gizliliğinin korunması gereken hâller bakımından risk teşkil edebilecek niteliktedir.

Yazılım: Talep edilen yazılımın veya yazılıma ilişkin kaynak kodların verilmesinin kaynak kod sahibi ile yapılan sözleşme aykırılık oluşturma riskinin olması, söz konusu kaynak kodun verilmesi hâlinde 5846 sayılı Fikir ve Sanat Eserleri Kanunu bakımından ihlallerin doğabileceği, öte yandan kodların devri ve saklanması sürecinde yetkili mercilerin ve denetim görevlilerinin söz konusu kodu uygun koşullarda saklayıp saklamayacağı bakımından soru işaretleri yaratmaktadır. Elbette birçok sözleşmede talep edilecek bilgi belgelerin yetkili kamu kurum ve kuruluşlar ile paylaşılması istisnai düzenleme olarak yer almaktadır. Ancak buradaki asıl problem yazılıma ilişkin bilgilerin paylaşılmasından ziyade, paylaşım konu yazılım/kaynak kodun uygun koşullarda saklanıp saklanmadığı hâlidir. Öte yandan bir sözleşmede Türk Hukuku dışında bir hukukun uygulanacağı belirlendiyse de sözleşmeye aykırılık hâlleri gündeme gelebilecektir.

Veri: Talep edilen verinin ticari sır ihtiva etmesi ve avukat-müvekkil gizliliğinin korunması gereken hâller bakımından risk teşkil edebilecek niteliktedir.

Donanım: Burada özellikle bir donanımın talep edilmesi hâlinde donanımla bütünleşik appliance yazılım olması hâlinde talep edilen donanım dışında appliance yazılıma da erişimin olması hâlinde ve appliance yazılıma erişim verilmemesi durumunda suçun oluşup oluşmayacağı tartışma konusu olabilecektir.

Talebin yerine getirilme süresi bakımından: Söz konusu maddede talep edilen bilgi, belge, yazılım, veri ve donanımın ne kadar sürede teslim edilmesi gerektiğine dair bir detay bulunmamaktadır. Bu durumda özellikle maddede suçun ikinci unsuru olarak nitelendirebileceğimiz “bilgi, belge, yazılım, veri ve donanımın” ne kadar süre içerisinde verilmesi gerektiği, veya talep edilen kişinin/kurumun söz konusu bilgi, belge, yazılım, veri ve

³ **Kaya**, Mehmet Bedii; *Siber Güvenlik Hukuku*, s. 325.

donanımı vermeye yetkili olup olmadığı durumlarda, örneğin şirket yetkilisinin denetim sırasında bulunmaması hâllerinde suçun oluşup oluşmayacağı belirsizlik barındırmaktadır.

Yaptırım bakımından: Maddede hem 1 yıldan 3 yıla kadar hapis cezası hem de 500 günden 1500 güne kadar adli para cezası düzenlenmiş olup, özellikle NIS2 Direktifi'nin idari para cezalarını düzenleyen 34. maddesinden ilham alınmak suretiyle yalnızca idari para cezası uygulanmasına dair düzenleme yapılması öngörülebilir. NIS2'nin 34. Maddesi aynı zamanda Direktif'in ihlali halinde uygulanacak idari para cezalarının her bir olay bakımından tüm koşulların dikkate alınmak suretiyle, etkili, orantılı ve caydırıcı olmasını sağlamayı öngörmüş olup, yalnızca idari para cezası düzenlemiştir. Bu bakımdan hapis cezası ve adli para cezası uygulamak yerine kademeli para cezası düzenlemesi değerlendirilebilir.

4. Alternatif Hüküm

Yukarıda değerlendirdiğimiz tüm riskleri göz önünde aldığımızda; sınırları belli, orantılı, tek yaptırımı olan ve daha detaylandırılmış bir hükmün varlığı değerlendirilebilir. Bu kapsamda hazırladığım alternatif hüküm şu şekildedir:

“Cezai hükümler ve idari para cezaları

MADDE 16- (1) *Bu Kanunla yetkilendirilen mercilerin ve denetim görevlilerinin, denetim amacıyla sınırlı ve orantılı biçimde, yazılı olarak ve makul süre tanıyarak talep ettikleri bilgi, belge, yazılım, veri ve donanımı kamu kurum ve kuruluşları hariç olmak üzere haklı bir neden olmaksızın vermeyenler veya haklı bir neden olmaksızın bunların alınmasına engel olanlar; talep edilen bilgi, belge, yazılım, veri ve donanımın önemi dikkate alınmak suretiyle beşyüz bin Türk lirasından beş milyon Türk lirasına kadar idari para cezası ile cezalandırılır.”*

5. Sonuç

Son yıllarda ülkemizde siber güvenlik alanında önemli düzenlemeler ve gelişmeler olmakla birlikte, her bir düzenlemenin; özellikle teknolojik gelişmeler ve hukuki düzlem dikkate alınarak ve orantılılık, hukuki güvenlik ilkesi ve uluslararası düzenlemeler kapsamında düzenlenmesi, bilişim hukuku perspektifinde etraflıca değerlendirilerek yapılması önem arz etmektedir. Bu kapsamda Kanunu'nun 16. maddesinin 1. fıkrası, önemli bir düzenleme olmakla birlikte, hükmün

belirsizliđi sebebiyle çeřitli sorunlar barındırmaktadır. Bu sorunların giderilmesi amacıyla hazırlanan alternatif hüküm; talebin denetim amacıyla sınırlı ve orantılı olması zorunluluđunu, makul süre güvencesini ve ihlalin ađırlıđına göre idari para cezaların belirlenmesini dikkate alarak düzenlenmiř olup, hem denetim mekanizmasının etkinliđini hem de denetlenlerin hukuki güvenliđini korumayı amaçlamaktadır.

6. Kaynakça ve Mevzuat

- KAYA, Mehmet Bedii; *Siber Güvenlik Hukuku*, 2026.
- KARAKEHYA, Hakan; USLUADAM, Asena Kamer; "Türk Ceza Hukuku Öğretisinde Suçun Manevi Unsuru Bağlamında Suç Genel Teorisine İliřkin Görüşler", *Dergipark*.
- ŞENOL, Cem; "7545 Sayılı Siber Güvenlik Kanunu'nda Düzenlenen Suçlar", *Türkiye Adalet Akademisi Dergisi*, Yıl 16, Sayı 63, Temmuz 2025.
- *7545 Sayılı Siber Güvenlik Kanunu*, RG. 19.03.2025/32846.
- *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, OJ L 333, 27.12.2022.