

Sır Saklama Yükümlülüğünü İhlal Suçu

Av. Burak Üçüncü · 6 Haziran 2026 · 9 dk okuma

7545 sayılı Siber Güvenlik Kanunu, [Siber Güvenlik Başkanlığı](#) bünyesinde yürütülen faaliyetler kapsamında edinilen bilgilerin gizliliğine büyük önem atfetmektedir. Bu önemi somutlaştıran düzenlemelerden biri, Kanun'un 13. maddesinde yer alan sır saklama yükümlülüğüdür. Bu yükümlülüğe aykırılık ise 16. maddenin üçüncü fıkrasında bağımsız ve ağır yaptırımlı bir suç tipi olarak düzenlenmiştir.

Madde metni son derece kısa ve nettir:

"Sır saklama yükümlülüğünü yerine getirmeyenlere dört yıldan sekiz yıla kadar hapis cezası verilir."

Bu fıkranın referans aldığı 13. madde ise şöyledir:

"Başkanlık tarafından yürütülen görev ve faaliyetler kapsamında edinilen kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgiler, kişisel veriler, ticari sırlar ve bunlara ait belgeler mevzuat gereği yetkili kılınan mercilerden başkasına açıklanamaz, gerçek ve tüzel kişilerin menfaatine kullanılamaz."

Dört yıldan sekiz yıla kadar hapis cezası öngörülmüş olması, bu suçu Kanun'daki en ağır suç tiplerinden biri haline getirmektedir. [Siber güvenlik kanunundaki suçlar](#) arasında, milli güce yönelik siber saldırı suçunun (m.16/6) ardından, Kanun'un en yüksek alt sınıra sahip ikinci suç tipidir. Bu ağırlık, Başkanlık bünyesinde edinilen bilgilerin niteliği düşünüldüğünde anlaşılabilir bir tercihtir: Başkanlık, görevleri gereği kritik altyapılara, devlet sırlarına, kişisel verilere ve ticari sırlara doğrudan erişim imkanına sahiptir. Bu bilgilerin yetkisiz kişilere ifşa edilmesi, telafisi güç zararlar doğurabilir.

BÖLÜM I

Korunan Hukuki Değer

Bu suç tipiyle korunan hukuki değer çok katmanlıdır.

Birinci katmanda, **Başkanlığın faaliyetlerinin güvenilirliği ve etkinliği** yer almaktadır. Siber güvenlik alanında görev yapan bir kurumun, kendisine tevdi edilen bilgilerin gizliliğini koruyamaması, tüm sisteme duyulan güveni temelden sarsacaktır. Kamu kurum ve kuruluşları ile özel sektör kuruluşlarının Başkanlıkla bilgi paylaşma konusundaki istekliliği, büyük ölçüde bu bilgilerin güvende tutulacağına duydukları inanca bağlıdır.

İkinci katmanda, **kişisel verilerin korunması hakkı** bulunmaktadır. Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan bu hak, Başkanlık bünyesinde işlenen kişisel veriler bakımından da geçerlidir. Kanun'un 6. maddesinin ikinci fıkrası, Başkanlık tarafından yürütülen işlemler kapsamındaki kişisel

verilerin hukuka uygun şekilde işlenmesini ve amacın ortadan kalkması halinde silinmesini zorunlu kılmaktadır.

Üçüncü katmanda ise **ticari sırların korunması** yer almaktadır. Başkanlığın denetim ve inceleme faaliyetleri sırasında özel sektör kuruluşlarının ticari sırlarına, iş süreçlerine, müşteri verilerine ve know-how bilgilerine erişmesi kaçınılmazdır. Bu bilgilerin ifşası, ilgili kuruluşlar bakımından ciddi rekabet dezavantajlarına yol açabilir.

Son olarak, **milli güvenlik** de korunan hukuki değerler arasında sayılmalıdır. Başkanlığın kritik altyapılar, savunma sanayi ve kamu kurumlarının bilişim sistemleri hakkında edindiği bilgiler, doğrudan milli güvenlikle ilişkilidir.

BÖLÜM II

Suçun Maddi Unsurları

A. Fail

Bu suç, özgü suç niteliğindedir. Yalnızca sır saklama yükümlülüğü bulunan kişiler tarafından işlenebilir.

Kanun'un 13. maddesi, sır saklama yükümlülüğünün kapsamını "Başkanlık tarafından yürütülen görev ve faaliyetler kapsamında edinilen" bilgilerle sınırlamıştır. Dolayısıyla bu yükümlülüğün ve buna bağlı cezai sorumluluğun muhatabı, Başkanlık faaliyetleri kapsamında bilgi edinme imkanına sahip olan kişilerdir. Bunlar arasında şu kişi grupları sayılabilir:

Başkanlık personeli:

Kadrolu veya sözleşmeli statüde çalışan tüm personel, görevleri süresince ve sonrasında sır saklama yükümlülüğüne tabidir. Kanun'un 12. maddesinin ikinci fıkrasında, Başkanlıktaki görev ve faaliyetler kapsamında edinilen bilgilerin yayımlanmasının veya açıklanmasının yasak olduğu ayrıca düzenlenmiştir.

Geçici görevlendirilenler:

Kanun'un 10. maddesinin ikinci fıkrası uyarınca, Başkanlıkta geçici olarak görevlendirilen personel de dahil olmak üzere görev alan tüm personele güvenlik soruşturması ve arşiv araştırması yapılmaktadır. Bu kişiler de sır saklama yükümlülüğüne tabidir.

Bağımsız denetçiler ve denetim kuruluşları:

Kanun'un 8. maddesinin birinci fıkrası uyarınca Başkanlık tarafından yetkilendirilen ve denetim faaliyetlerinde görev alan bağımsız denetçi ve kuruluşlar, denetim sırasında edindikleri bilgiler bakımından sır saklama yükümlülüğü altındadır.

Kurul üyeleri ve komisyon çalışanları:

Siber Güvenlik Kurulu'nun toplantılarına katılan üyeler ve Kanun'un 9. maddesinin üçüncü fıkrası uyarınca oluşturulan komisyon ve çalışma gruplarında görev alan kişiler de bu yükümlülüğün muhatabıdır.

Suçun özgü suç niteliği, iştirak bakımından önem taşımaktadır. Sır saklama yükümlülüğü bulunmayan bir kişi, bu suçun doğrudan faili olamaz; ancak TCK'nın 40. maddesi uyarınca azmettiren veya yardım eden sıfatıyla suça iştirak edebilir.

B. Mağdur

Suçun mağduru, ifşa edilen bilginin niteliğine göre farklılaşır. Kişisel verilerin ifşası halinde ilgili gerçek kişi, ticari sırların ifşası halinde ilgili kuruluş, gizlilik taşıyan kamu bilgilerinin ifşası halinde ise devlet mağdur konumundadır. Her durumda, Başkanlığın kurumsal güvenilirliği de zarar görmektedir.

C. Fiil

Suçun maddi unsurunu oluşturan fiil, sır saklama yükümlülüğünün yerine getirilmemesidir. Bu, 13. madde ile birlikte değerlendirildiğinde iki seçimlik hareket ortaya çıkmaktadır:

Birinci seçimlik hareket, gizlilik taşıyan bilgilerin, kişisel verilerin, ticari sırların ve bunlara ait belgelerin mevzuat gereği yetkili kılınan merciler dışında başkasına *açıklanmasıdır*. Açıklama, sözlü, yazılı veya elektronik ortamda gerçekleştirilebilir. Bilginin tek bir kişiye ifşa edilmesi yeterlidir; alenileştirilmesi zorunlu değildir.

İkinci seçimlik hareket, bu bilgilerin gerçek ve tüzel kişilerin *menfaatine kullanılmasıdır*. Bu hareket, bilginin üçüncü kişilere açıklanmasını zorunlu kılmaz. Failin, edindiği gizli bilgiyi kendi menfaatine veya belirli bir kişi ya da kuruluşun menfaatine kullanması yeterlidir. Örneğin, bir Başkanlık personelinin denetim sırasında öğrendiği bir şirketin siber güvenlik açığını, bu bilgiyi açıklamaksızın rakip şirketle iş ilişkisi kurmak amacıyla kullanması, ikinci seçimlik hareket kapsamında değerlendirilebilir.

D. Suçun Konusu

Suçun konusunu oluşturan bilgi ve belgeler, 13. maddede dört kategori halinde sayılmıştır:

- Gizlilik taşıyan bilgiler:** Başkanlık faaliyetleri kapsamında edinilen ve kamuya açık olmayan her türlü bilgidir. Devlet sırrı niteliğindeki bilgiler de bu kapsamdadır.
- Kişisel veriler:** 6698 sayılı Kişisel Verilerin Korunması Kanunu anlamında kişisel veri niteliği taşıyan her türlü bilgidir.
- Ticari sırlar:** Denetlenen kuruluşların rekabet avantajı sağlayan, kamuya açık olmayan iş bilgileri, müşteri verileri, algoritmaları, iş süreçleri ve benzeri bilgilerdir.
- Bunlara ait belgeler:** Yukarıdaki kategorilerdeki bilgileri içeren fiziksel veya dijital belgelerdir.

BÖLÜM III —

Suçun Manevi Unsuru

Kanun'da özel bir kast türü aranmamıştır; dolayısıyla genel kast yeterlidir. Failin, açıkladığı veya menfaatine kullandığı bilginin gizlilik taşıdığını bilmesi ve buna rağmen sır saklama yükümlülüğüne aykırı davranması gerekmektedir.

Taksirle işlenme hali düzenlenmemiştir. Bu nedenle, güvenlik ihlali sonucu bilgilerin istem dışı olarak ifşa edilmesi (örneğin, bir Başkanlık personelinin dizüstü bilgisayarının çalınması sonucu verilerin ele geçirilmesi) bu suçu oluşturmayacaktır. Ancak bu durumda, failin güvenlik önlemlerini almadaki ihmali, TCK'nın 257. maddesindeki ihmali davranışla görevi kötüye kullanma veya Kanun'un 16. maddesinin dokuzuncu fıkrasındaki görevi kötüye kullanma suçu bakımından ayrıca değerlendirilebilir.

Olası kast bakımından ise failin, belirli bir bilgiyi paylaşmasının sır saklama yükümlülüğünü ihlal edebileceğini öngörmesine rağmen bu sonucu göze alarak davranması halinde suçun oluşacağı kabul edilmelidir.

BÖLÜM IV —

Yaptırım

Suç için öngörülen yaptırım, dört yıldan sekiz yıla kadar hapis cezasıdır. Dikkat çekici olan husus, bu suçta adli para cezasının öngörülmemiş olmasıdır. Kanun koyucu, salt hapis cezası öngörmek suretiyle bu suçun ciddiyetini vurgulamıştır.

Alt sınırın dört yıl olması, uygulamada son derece önemli sonuçlar doğurmaktadır:

Hükmün açıklanmasının geri bırakılması (HAGB):

CMK'nın 231. maddesi uyarınca HAGB, hükmedilen cezanın iki yılı aşmaması koşuluna bağlıdır. Alt sınırın dört yıl olması nedeniyle, bu suçta HAGB uygulanması mümkün değildir.

Cezanın ertelenmesi:

TCK'nın 51. maddesi uyarınca, iki yıl ve altındaki hapis cezaları ertelenebilir. Alt sınırın dört yıl olması nedeniyle, erteleme de mümkün değildir.

Kısa süreli hapis cezasının seçenek yaptırımlara çevrilmesi:

TCK'nın 49. maddesi uyarınca kısa süreli hapis cezası bir yıl ve altındaki cezaları kapsamaktadır. Bu suçta uygulama alanı bulunmamaktadır.

Tutuklama:

CMK'nın 100. maddesi uyarınca, üst sınırı iki yılı aşan suçlarda tutuklama kararı verilebilir. Bu suçun üst sınırının sekiz yıl olması nedeniyle, soruşturma ve kovuşturma aşamalarında tutuklama kararı verilebilecektir.

Sonuç olarak, bu suçun failinin mahkum olması halinde cezaevine girmesi kaçınılmaz görünmektedir. Bu durum, sır saklama yükümlülüğünün ne denli ciddi bir sorumluluk olduğunu açıkça ortaya koymaktadır.

BÖLÜM V —

Nitelikli Haller

Kanun'un 16/7 hükmü bu suç bakımından da uygulanacaktır:

Kamu görevlisi tarafından işlenmesi: Bu suçun doğası gereği, failerin büyük çoğunluğunun kamu görevlisi sıfatını taşıması muhtemeldir. Başkanlık personeli, kamu görevlisi statüsündedir. Bu nitelikli halin uygulanması halinde alt sınır beş yıl dört aya, üst sınır ise on yıl sekiz aya yükselmektedir.

Birden fazla kişi tarafından birlikte işlenmesi: Birden fazla Başkanlık personelinin koordineli şekilde gizli bilgileri ifşa etmesi bu kapsamda değerlendirilecektir. Alt sınır altı yıla, üst sınır on iki yıla yükselmektedir.

Bir örgütün faaliyeti çerçevesinde işlenmesi: Özellikle yabancı istihbarat servisleri veya organize suç örgütleri adına bilgi sızdırma hallerinde bu nitelikli hal uygulanacaktır. Cezanın yarısından iki katına kadar artırılması, alt sınırın altı yıla, üst sınırın ise on altı yıla çıkması anlamına gelmektedir.

TCK'daki Benzer Suçlarla İlişkisi

A. TCK m.239 – Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması

TCK'nın 239. maddesinde düzenlenen ticari sır ifşası suçu ile Kanun'un 16/3 hükmü arasında önemli bir ilişki bulunmaktadır. Başkanlık faaliyetleri kapsamında edinilen ticari sırların açıklanması, her iki suçun unsurlarını da karşılayabilir. Bu durumda, özel norm-genel norm ilişkisi çerçevesinde Kanun'un 16/3 hükmünün öncelikle uygulanması gerekecektir.

B. TCK m.258 – Göreve İlişkin Sırrın Açıklanması

TCK'nın 258. maddesinde düzenlenen göreve ilişkin sırrın açıklanması suçu, kamu görevlilerinin görevleri nedeniyle öğrendikleri sırları ifşa etmesini cezalandırmaktadır. Başkanlık personelinin sır saklama yükümlülüğünü ihlal etmesi, hem bu suçun hem de Kanun'un 16/3 hükmünün unsurlarını karşılayabilir. Bu durumda yine özel norm olan Kanun'un 16/3 hükmü uygulanacaktır. Kanun'un öngördüğü cezanın (4-8 yıl) TCK m.258'deki cezadan (1-4 yıl) çok daha ağır olduğu da not edilmelidir.

C. TCK m.329-339 – Devlet Sırlarına Karşı Suçlar ve Casusluk

Başkanlık bünyesinde edinilen bilgilerin devlet sırrı niteliği taşıması ve bunların yabancı devlet veya örgüt lehine ifşa edilmesi halinde, TCK'nın yedinci bölümünde düzenlenen devlet sırlarına karşı suçlar ve casusluk hükümleri gündeme gelebilir. Bu durumda, Kanun'un 16/6 hükmündeki tali norm kaydının (m.16/3 bakımından mevcut olmayan) bulunmaması, fikri içtima kurallarının uygulanmasını zorunlu kılacaktır. TCK'nın 44. maddesi uyarınca en ağır cezayı gerektiren suçtan ceza verilecektir.

Uygulamada Karşılaşılabilecek Sorunlar

A. Yükümlülüğün Süresinin Belirsizliği

Kanun'un 13. maddesi, sır saklama yükümlülüğünün ne kadar süreyle devam edeceğini düzenlememektedir. Kanun'un 12. maddesindeki iki yıllık yasak süresinin sır saklama yükümlülüğü için de geçerli olup olmadığı açık değildir. Sır saklama yükümlülüğünün niteliği gereği süresiz olması gerektiği ileri sürülebilir; zira bilginin gizlilik niteliği zamanla ortadan kalksa dahi, bazı bilgiler (özellikle milli güvenlikle ilgili olanlar) kalıcı olarak gizli kalma gerekliliği taşımaktadır.

B. Gizlilik Derecesinin Belirlenmesi

Kanun'un 13. maddesi "gizlilik taşıyan bilgiler" ifadesini kullanmakla birlikte, hangi bilgilerin gizlilik taşıdığına ilişkin bir sınıflandırma yapmamıştır. Bilginin gizli olup olmadığının tespitinde, bilginin niteliği, kamuya açık olup olmadığı ve açıklanmasının yaratacağı zarar potansiyeli gibi ölçütler kullanılabilir. Ancak bu ölçütlerin somut olayda uygulanması, failin eyleminin suç oluşturup oluşturmadığının belirlenmesinde belirsizliklere yol açabilir.

C. Basın ve İfade Özgürlüğü ile Çatışma

Başkanlık faaliyetleri kapsamında edinilen bilgilerin, kamu yararı gerekçesiyle basına sızdırılması halinde, sır saklama yükümlülüğü ile basın özgürlüğü ve halkın bilgilendirilme hakkı arasında bir gerilim ortaya çıkabilir. Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü ve 28. maddesindeki basın özgürlüğü, bu bağlamda değerlendirilmelidir. Ancak özellikle milli güvenlikle doğrudan ilişkili bilgiler bakımından, bu özgürlüklerin sınırlandırılmasının meşru olacağı kabul edilmektedir.

D. İhbarcılık Sorunu

Başkanlık bünyesinde hukuka aykırı uygulamaların varlığını tespit eden bir personelin, bu durumu yetkili makamlara veya kamuoyuna bildirmesi halinde sır saklama yükümlülüğünü ihlal edip etmediği tartışmalıdır. Türk hukukunda henüz kapsamlı bir ihbarcı koruma mevzuatı bulunmaması, bu sorunu daha da karmaşık hale getirmektedir. Bununla birlikte, suç ihbarının hukuka uygunluk sebebi oluşturacağı ve bu kapsamda yapılan bildirimlerin sır saklama yükümlülüğünü ihlal etmeyeceği genel kabul görmektedir.

BÖLÜM VIII

Sonuç

7545 sayılı Siber Güvenlik Kanunu'nun 16. maddesinin üçüncü fıkrasında düzenlenen sır saklama yükümlülüğünü ihlal suçu, Kanun'un en ağır yaptırımlarından birini içermektedir. Alt sınırın dört yıl olarak belirlenmesi, HAGB ve erteleme gibi müesseselerin uygulanmasını imkansız kılmakta ve mahkum olan failin cezaevine girmesini kaçınılmaz hale getirmektedir.

Bu ağırlık, Başkanlık bünyesinde edinilen bilgilerin hassasiyetiyle doğrudan orantılıdır. Kritik altyapı bilgileri, kişisel veriler, ticari sırlar ve milli güvenlikle ilgili verilerin korunması, siber güvenlik sisteminin bütünlüğü bakımından yaşamsal öneme sahiptir.

Bununla birlikte, gizlilik derecesinin belirlenmesi, yükümlülüğün süresi, ifade özgürlüğü ile denge ve ihbarcılık gibi konularda Kanun'un ortaya çıkardığı boşlukların içtihatlarla ve ikincil mevzuatla doldurulması gerekmektedir. Özellikle Başkanlık personeline yönelik gizlilik politikalarının ve bilgi sınıflandırma kriterlerinin açık ve anlaşılır şekilde belirlenmesi, hem personelin cezai sorumluluk riskini net olarak görmesi hem de yükümlülüğün etkin şekilde uygulanabilmesi bakımından büyük önem taşımaktadır.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/sir-saklama-yukumlulugunu-ihlal-sucu>