

Siber Güvenlik Hukukunda Yeni Rejim: Siber Güvenlik Kanunu

28 Mart 2025

Meclise sunulmasından yaklaşık iki ay sonra kabul edilen [Siber Güvenlik Kanunu](#) ("**Kanun**"), 19 Mart 2025'te Resmî Gazetede yayımlanarak yürürlüğe girdi. Peki Kanun kimleri ilgilendiriyor? Kanun, siber ekosistemi nasıl etkiliyor, mevcut düzende neleri değiştiriyor? Kanun'da özellikle özel sektörü ilgilendiren düzenlemeler neler? Bunları ve Kanun'da düzenlenen, önemli bulduğumuz diğer bazı hususları sizler için özetledik.

1. Daha Önce Bir Siber Güvenlik Hukuku Yok muydu?

Siber güvenlik uzun yıllardır Türkiye'nin politika alanında önemli bir yere sahip. Kanun da Türkiye'de siber güvenliğe ilişkin ilk ve tek hukuki düzenleme değil.

Örneğin, 6 Temmuz 2019 tarihli ve 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ve bununla bağlantılı Bilgi ve İletişim Güvenliği Rehberi, siber güvenlikle ilgili çeşitli önlemler almayı zorunlu kılıyordu ancak bu düzenlemeler, kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmeleri kapsıyordu.

Daha fazla kişi ve kurumu kapsayan Kişisel Verilerin Korunması Kanunu ("**KVKK**"), veri sorumlusu ve veri işleyenlere veri güvenliğini sağlama yükümlülüğü getirmiş olsa da KVKK, sadece "kişisel verilere" yönelik hukuki çerçeveyi oluşturuyor.

Bunların yanında, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik gibi çeşitli sektörel düzenlemelerde siber güvenlik ile ilişkili hükümler mevcuttu. Kanun, bu şekilde dağınık düzenlenmiş bir alanda daha genel ve kapsamlı düzenlemeler (Kanun'un gerekçesinin deyimıyla bir "çatı mevzuat") için yasal zemini sağlıyor.

Bu noktada belirtmekte fayda var: Kanun'un uygulanması ile ilgili ikincil düzenlemeler yapıncaya kadar mevcut düzenlemeler, Kanun'a uygun olduğu ölçüde yürürlükte kalmaya devam edecek.

2. Kanun'daki Düzenlemeler Kimleri Kapsıyor?

Her kişi ve kurumun, bilişim ağlarıyla ilgili her türlü işleminin Kanun kapsamına girdiğini söylersek mübalağa etmiş olmayız. Zira Kanun'un kapsadığı kişi ve kurumlar şu şekilde belirlenmiş: "**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 kuruluşlar".

Ayrıca burada geçen "siber uzay" ifadesinin de: "**doğrudan ya da dolaylı olarak** internete, elektronik haberleşme veya bilgisayar ağlarına bağlı olan **tüm** bilişim sistemleri ve bunları birbirine bağlayan ağlardan oluşan ortam" olmak üzere çok geniş bir tanıma sahip olduğunu hemen belirtelim.

Sadece millî güvenlikle ilgili çeşitli kanunların kapsamındaki faaliyetler, bu Kanun'un kapsamının dışında tutulmuş (Bunlar: Polis Vazife ve Salâhiyet Kanunu, Sahil Güvenlik Komutanlığı Kanunu, Jandarma Teşkilat, Görev ve Yetkileri Kanunu, Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu, Türk Silahlı Kuvvetleri İç Hizmet Kanunu).

3. Yeni Rejim: Siber Güvenlik Başkanlığı ve Siber Güvenlik Kurulu

Kanun teklifinin meclise sunulmasından iki gün önce, [Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi](#) ("Kararname") Resmî Gazetede yayımlanmış ve Siber Güvenlik Başkanlığı ("**Başkanlık**") kurulmuştu. Kararname, Cumhurbaşkanlığı bünyesindeki ve bugün itibarıyla kapatılan Dijital Dönüşüm Ofisinin siber güvenlik hakkında çalışmalar yapmakla ilgili görevlerini yeni kurulan Başkanlığa aktarıyor ve Başkanlığın bazı görev ve yetkilerini tanımlıyordu. Burada belirtilen yetki ve görevler, siber güvenlik hakkında stratejileri belirlemek ve çeşitli çalışmalar yürütmekten ibaretti.

Kanun ise Bilgi Teknolojileri ve İletişim Kurumunun ("**BTK**") siber saldırıların tespiti ve önlenmesi ile ilgili yetkilerini ve Ulaştırma ve Altyapı Bakanlığının siber güvenlikle ilgili düzenleyici yetkilerini Başkanlığa devrediyor ve böylece Başkanlığı, siber güvenlik alanında yetkili temel kuruluş hâline getiriyor.

Kanun ile Cumhurbaşkanı'nın başkanlık edeceği bir Siber Güvenlik Kurulu ("**Kurul**") da kuruluyor. Kurul'un daha çok yol haritası belirleme ve politika, eylem planı gibi stratejik konularda ve düzenleyici işlemlerin yapılmasında karar alma gibi bir rolü olduğu söylenebilir.

Kanun sadece mevcut kurumların siber güvenlikle ilgili görev ve yetkilerini Başkanlık bünyesinde birleştirmekle kalmıyor. Bunların yanında, Başkanlığa kritik sistemlerin korunması, siber saldırıların tespiti, önlenmesi, bu saldırılara müdahale edilmesi ile yerli ve milli siber güvenlik çözümlerinin geliştirilmesi ve uygulanması başta olmak üzere geniş bir misyon yükleniyor.

Başkanlığa siber saldırılaresnası ve sonrası ile ilgili çeşitli yetkiler de veriliyor. Böylece, siber saldırılarla mücadele ve siber dayanıklılığın artırılması alanında da aktif rol almasının beklendiği görülüyor.

Kanun'un Başkanlığa tanıdığı en önemli yetki ise "siber güvenlik denetimini gerçekleştirmek ve sonucuna göre yaptırım uygulamak". Aşağıda bu yetkiyi detaylı olarak değerlendirdik.

4. Başkanlığın Denetim Yetkisi

Kanun, Başkanlığa çok geniş bir denetim yetkisi veriyor. Buna göre Başkanlık, Kanun'un kapsamına giren bütün işlem ve fiilleri denetleyebilecek. Yukarıda da değindiğimiz üzere Kanun siber uzayda varlık gösteren neredeyse her organizasyonu kapsadığı için, Başkanlığın her türlü kişi ve kurumun bilişim ağlarıyla ilgili neredeyse her türlü işlemi denetleyebileceğini söylemek mümkün.

Denetim kapsamında Başkanlığa yerinde inceleme yapma yetkisi de verilmiş. Bu kapsamda denetimle görevlendirilenlerin yapabileceği işlemler şu şekilde sayılmış: 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. Bu çerçevede, denetimle yükümlü kişilere fiili olarak Rekabet Kurumuna benzer yetkilerin tanındığı görülmüyor.

Başkanlığa konutta, iş yerinde ve kamuya açık olmayan kapalı alanlarda arama yapma ve bu kapsamda kopya çıkarma ve el koyma yetkisi de tanınmış ancak bu, “millî güvenlik, kamu düzeni, suç işlenmesinin veya siber saldırıların önlenmesi” amaçlarıyla sınırlı tutulmuş ve hâkim kararı veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emri bulunması şartına bağlanmış.

5. Yükümlülükler ve Yaptırımlar

Kanun, Başkanlığa tanıdığı yetkilerle paralel olarak, faaliyetlerinde bilişim sistemlerini kullanan kişi ve kurumlara çeşitli yükümlülükler öngörüyor:

- Başkanlığın görev ve faaliyetleri kapsamında talep ettiği **her türlü veri, bilgi, belge, donanım, yazılım ve diğer her türlü katkıyı Başkanlığa iletmek**. Bu yükümlülüğe aykırı biçimde veri, bilgi, belge ve donanımı vermemenin veya bunların alınmasına engel olmanın, **bir yıldan üç yıla kadar hapis ve beş yüz günden bin beş yüz güne kadar adli para cezası** ile cezalandırılacağı belirlenmiş.
- Başkanlığın denetimine tabi tutulma durumunda ilgili cihaz, sistem, yazılım ve donanımları verilen sürede denetlemeye açık tutmak, denetim için gerekli altyapıyı temin etmek ve çalışır vaziyette tutmak için gerekli önlemleri almak. Bu yükümlülüğe aykırılık için ise **100.000 – 1.000.000 TL arasında idari para cezası** öngörülmüş ancak bu yükümlülüğün **ticari şirketler** tarafından yerine getirilmemesi halinde, idari para cezasının **“100.000 TL’den az olmamak üzere bağımsız denetimden geçmiş yıllık finansal tablolarında yer alan brüt satış hasılatının %5’ine kadar”** olacağı belirlenmiş.
- Siber güvenlikle ilgili mevzuatta öngörülen tedbirleri almak. Bu yükümlülüğe aykırılık için **1.000.000 – 10.000.000 TL arasında idari para cezası** öngörülmüş.
- Faaliyet gösterilen alanda tespit edilen zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmek. Bu bildirim yükümlülüğüne aykırılık halinde ise **1.000.000 – 10.000.000 TL arasında idari para cezası** uygulanacağı öngörülmüş.
- *Kamu kurum ve kuruluşları ile kritik altyapılarda* kullanılacak siber güvenlik ürün, sistem ve hizmetleri Başkanlık tarafından yetkilendirilmiş ve belgelendirilmiş siber güvenlik uzmanlarından, üreticilerden veya şirketlerden tedarik etmek. Bu

yükümlülüğe aykırı davranılması halinde **1.000.000 – 10.000.000 ₺ idari para cezası** öngörülmüş.

Bunların yanında, siber olgunluğun artırılmasına yönelik Başkanlık tarafından geliştirilen düzenleyici işlemlerde yer alan hususları yerine getirmek ve gerekli tedbirleri almak gibi bir yükümlülük de öngörülmüş; fakat, Kanun'da bu yükümlülüğü yerine getirmeyenler için bir yaptırıma yer verilmiyor.

Son olarak, Kanun'da siber güvenlik şirketlerine ve Başkanlık personeline özgü yükümlülükler ve bunlar için öngörülmüş yaptırımların da yer aldığını belirtelim.

6. Ve Diğer Cezalar...

Yukarıda değindiğimiz yaptırımların yanında Kanun, siber güvenlik alanında çeşitli yeni suçlar da tanımlıyor. Başlıcaları şu şekilde sayılabilir:

- Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren unsurlarına yönelik olarak siber saldırıda bulunmak veya bu saldırı neticesinde elde edilen her türlü veriyi siber uzayda bulundurmak (fiil daha ağır bir cezayı gerektiren başka bir suç oluşturmadığı takdirde **sekiz yıldan on iki yıla kadar hapis cezası**)
- Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren unsurlarına yönelik yapılan siber saldırının sonucunda elde edilen verinin siber uzayda yayılması, başka bir yere gönderilmesi ve satışa çıkarılması (**on yıldan on beş yıla kadar hapis cezası**)
- Hâlihazırda sızmış olan kişisel verilerin veya kritik kamu hizmeti kapsamına giren kurumsal verilerin, izinsiz bir biçimde erişime açmak, paylaşmak veya satışa çıkarmak (**üç yıldan beş yıla kadar hapis cezası**)
- Veri sızıntısı olmadığı hâlde **halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef göstermek amacıyla** siber güvenlikle ilgili veri sızıntısı olduğuna yönelik **gerçeğe aykırı** içerik oluşturmak veya içeriği bu amaçla yaymak (**iki yıldan beş yıla kadar hapis cezası**)

Bu son saydığımız suçla ilgili düzenleme, Kanun teklifinin mecliste görüşülmesi esnasında kamuoyunda ve basın mecralarında birçok tartışmaya yol açmıştı. Kanun teklifinin ilk hâlinde çok geniş bir şekilde tanımlanmış olan bu suç, ilgili komisyonca görüşülme sürecinde her türlü faaliyeti değil, içerik oluşturma ve yayma faaliyetleri ile ve "halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef göstermek" kastıyla sınırlandırıldı ve Genel Kurulda da bu şekilde kabul edildi.

7. Sonuç

Siber güvenlik, Türkiye'deki mevcut düzenlemelerde yer almayan bir konu değil ancak bu konudaki mevcut düzenlemelerin dağınık olması ve düzenleme yetkisinin farklı kurumlarda

bulunması sebebiyle bütüncül ve tutarlı bir siber güvenlik mevzuatı oluşturulması mümkün olmamıştı. Daha önce bunun hedeflendiğini eylem planlarından ve çeşitli strateji belgelerinden biliyorduk; ancak, Kararname ile Başkanlığın kurulması ve Kanun ile temel bir düzenlemenin getirilmiş olması, şimdiye kadar bu yönde atılmış en büyük adım olarak görülebilir.

Kanaatimizce, siber güvenlik alanındaki hedeflere ulaşmak için mevzuatsal düzenlemelerin yapılması yeterli olmayacak, nasıl bir uygulama geliştirildiği de önem taşıyacaktır.

Her ne kadar düzenlemeler millî güvenlik odaklı ve dolayısıyla daha çok kamu kurum ve kuruluşlarını etkileyecek gibi gözükse de Kanun'da öngörülen yükümlülükler ve yaptırımlar ile Başkanlığın yetkileri göz önüne alındığında, ilerleyen süreçte özel sektörün de bu düzenlemelerden önemli bir şekilde etkileneceğini öngörmek mümkün.

Şimdilik Başkanlığın yapısı somut olarak kurulamadığı ve operasyonel hale gelmediği gibi henüz ikincil düzenlemelerin de bulunmaması nedeniyle bir geçiş döneminde olduğumuz söylenebilir. Yeni siber güvenlik hukukunun kimleri ne yönde etkileyeceğini çıkartılacak ikincil düzenlemelerin içerikleri fakat daha da önemlisi yeni kurulmuş olan Başkanlığın konuya yaklaşımı belirleyecek. Sizleri bu konularda bilgilendirmeye devam edeceğiz.

Bora Yazıcıoğlu
bora@yazicioglulegal.com

Aslı Rabia Savaş
asli@yazicioglulegal.com

Ferat Gümüş
ferat@yazicioglulegal.com

Bu not hukuki görüş niteliğinde değildir. Sadece bilgi amaçlı hazırlanmış ve gönderilmiştir.

Konuyla ilgili hukuki görüş almak isterseniz bizimle iletişime geçmenizi rica ederiz.