SİBER GÜVENLİK KANUNU

Kanun No. 7545		Kabul Tarihi: 12/3/20

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1- (1) Bu Kanunun amacı, Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel tehditlerin tespit ve bertaraf edilmesi, siber olayların muhtemel etkilerini azaltmaya yönelik esasların belirlenmesi, kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşların siber saldırılara karşı korunmasına yönelik gerekli düzenlemelerin yapılması, ülkenin siber güvenliğini güçlendirmek için strateji ve politikaların belirlenmesi ile Siber Güvenlik Kurulunun kurulmasına ilişkin esasları düzenlemektir.

Kapsam

MADDE 2- (1) Bu Kanun, 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 kuruluşları kapsar.

(2) 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu ve 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu uyarınca yürütülen istihbari faaliyetler ile 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ile 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu uyarınca yürütülen faaliyetler bu Kanun kapsamı dışındadır.

Tanım ve kısaltmalar

MADDE 3- (1) Bu Kanunda geçen;

a) Barındırma: Bilişim sistemlerinin harici bir veri merkezinde bulundurulmasını,

b) Başkan: Siber Güvenlik Başkanını,

c) Başkanlık: Siber Güvenlik Başkanlığını,

ç) Bilişim sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda kullanılan donanım, yazılım, sistem ve aktif veya pasif durumda bulunan tüm diğer bileşenleri,

d) Kritik altyapı: İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara ve güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları,

e) Kritik kamu hizmeti: Ulusal, toplumsal veya ekonomik faaliyetlerin sürdürülmesi için gerekli olan ve kesintiye uğraması veya zarar görmesi halinde ulusal güvenlik, ülkenin sosyal veya ekonomik refahı, kamu düzeni veya sağlığı ya da diğer hizmetlerin sunumu üzerinde önemli bir etki oluşturabilecek ülke genelinde tekel veya sınırlı ikame ile sunulan hizmeti,

f) Siber güvenlik: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki ve alarm mekanizmalarının devreye alınmasını ve sonrasında yaşanan siber olay öncesi duruma geri döndürülmesini kapsayan faaliyetler bütününü,

g) Siber olay: Bilişim sistemlerinin veya verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini,

ğ) Siber saldırı: Siber uzaydaki bilişim sistemlerinin ve bu sistemler tarafından işlenen verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi veya bilişim sistemlerine yönelik olarak kasıtlı yapılan işlemleri,

h) Siber tehdit: Bilişim sistemlerinin, bu sistemlerde bulunan veya bu sistemler tarafından işlenen verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesine neden olabilecek potansiyel tehlikeleri,

ı) Siber tehdit istihbaratı: Siber uzaydaki varlıklara yönelik mevcut veya potansiyel siber tehdit unsurları ile siber saldırılar hakkında bir araya getirilmiş, dönüştürülmüş, analiz edilmiş, yorumlanmış veya zenginleştirilmiş bilgiyi,

i) Siber uzay: Doğrudan ya da dolaylı olarak internete, elektronik haberleşme veya bilgisayar ağlarına bağlı olan tüm bilişim sistemlerini ve bunları birbirine bağlayan ağlardan oluşan ortamı,

j) SOME: Siber olaylara müdahale ekibini,

k) Varlık: Elektronik veya fiziksel ortamlarda yer alan ve iletişim yoluyla aktarılabilen veriyi içeren tüm bilgi ve bilgi işleme olanaklarını,

veriyi kullanan veya taşıyan personeli ve veriyi barındıran fiziksel mekânları,

l) Zafiyet: Siber uzayda yer alan varlıkların herhangi bir siber tehdit tarafından istismar edilebilecek zayıflık ve güvenlik açıklarını,

ifade eder.

Temel ilkeler

MADDE 4- (1) Siber güvenliğin sağlanmasında temel ilkeler şunlardır:

a) Siber güvenlik milli güvenliğin ayrılmaz bir parçasıdır.

b) Kritik altyapı ve bilişim sistemlerinin korunması ile güvenli bir siber uzay oluşturulması temel hedeftir.

c) Siber güvenlikle ilgili çalışmalar kurumsallık, süreklilik ve sürdürülebilirlik temelli yürütülür.

ç) Siber güvenlik tedbirlerinin, hizmet ve ürünlerin tüm yaşam döngüsü boyunca uygulanması esastır.

d) Siber güvenliğin sağlanmasına yönelik çalışmalarda öncelikle yerli ve milli ürünler tercih edilir.

e) Siber güvenlik politika ve stratejilerinin yürütülmesi ile siber saldırıların önlenmesi veya etkisinin azaltılmasına yönelik gerekli tedbirlerin alınmasından tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler sorumludur.

f) Siber güvenlik süreçlerinin yürütülmesinde hesap verebilirlik esastır.

g) Siber güvenlik politika ve strateji geliştirme çalışmaları sürekli gelişim yaklaşımı ile yürütülür.

ğ) Siber güvenlik alanında nitelikli insan kaynağı kabiliyet ve kapasitesinin artırılmasına yönelik çalışmalar teşvik edilir.

h) Siber güvenlik kültürünün toplum geneline yaygınlaştırılması hedeflenir.

ı) Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilir.

İKİNCİ BÖLÜM

Görev, Yetki, Sorumluluk, Denetim ve Siber Güvenlik Kurulu

Başkanlığın görevleri

MADDE 5- (1) Başkanlığın görevleri şunlardır:

a) İlgili mevzuatta yer alan görevleri yapmak.

b) Kritik altyapılar ve bilişim sistemlerinin siber dayanıklılığının artırılmasına, siber saldırılara karşı korunmasına, gerçekleştirilen siber saldırıların tespitine, muhtemel saldırıların önlenmesine ve etkilerinin azaltılmasına veya ortadan kaldırılmasına yönelik faaliyet yürütmek, bu kapsamda zafiyet ve sızma testleri ile varlıklara yönelik risk analizleri yapmak veya yaptırmak, siber tehditlerle mücadele etmek, siber tehdit istihbaratı elde etmek, oluşturmak ve paylaşmak, zararlı yazılım inceleme faaliyetleri yürütmek.

c) Kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek.

ç) Kamu kurum ve kuruluşları ile kritik altyapıların veri envanteri dâhil olmak üzere tüm varlıklarının envanterinin tutulmasını ve varlıklara yönelik risk analizinin gerçekleştirilmesini sağlamak, kamu kurum ve kuruluşları ile kritik altyapıların sahip olduğu varlıkların kritikliğine göre güvenlik tedbirlerini almak veya aldırmak.

d) SOME'ler kurmak, kurdurmak ve denetlemek, SOME'lerin olgunluk seviyelerinin belirlenmesi ve artırılması için çalışmalar yapmak, siber güvenlik tatbikatları gerçekleştirerek SOME'lerin siber olay müdahale kabiliyetlerini ölçmek, diğer ülkelerin siber olaylara müdahale ekipleriyle koordinasyon kurmak, her türlü siber müdahale aracının ve milli çözümlerin üretilmesi ve geliştirilmesi amacıyla çalışmalar yapmak, yaptırmak ve bunları teşvik etmek.

e) Siber güvenlik alanında faaliyet gösterenlerin uyması gereken usul ve esasları düzenlemek.

f) Kamu kurum ve kuruluşları ile kritik kamu hizmetlerinin siber güvenliğini sağlamak amacıyla gerekli altyapıları kurmak, kurdurmak, işletmek, işlettirmek ve kamu kurum ve kuruluşlarına güvenli sistem ve altyapılar üzerinden barındırma hizmeti sunmak veya sunulmasını sağlamak, bu faaliyetlere yönelik uygulama usul ve esaslarını belirlemek.

g) Siber güvenlik alanına ilişkin standartları hazırlamak, diğer kişi veya kuruluşlarca hazırlanan standartları tetkik etmek, bunlar hakkında mütalaa vermek, uygun bulduğu takdirde standart olarak kabul etmek, bunları yayımlamak ve uygulanmalarını takip etmek.

ğ) Siber güvenlik alanına ilişkin yazılım, donanım, ürün, sistem ve hizmetlere yönelik test ve sertifikasyon işlemlerini yürütmek, buna yönelik test altyapıları kurmak, kurdurmak ve işletmek ile siber güvenlik uzmanları ve şirketlerine yönelik sertifikasyon, yetkilendirme ve belgelendirme işlemlerini ilgili kurumlarla koordineli olarak yürütmek.

h) Siber güvenlik denetimini gerçekleştirmek ve sonucuna göre yaptırım uygulamak.

ı) Kamu kurum ve kuruluşları ile kritik altyapılarda kullanılacak siber güvenlik ürün ve hizmetleri ile bunları sağlayacak işletmelerin taşıması gereken niteliklere yönelik teknik kriterler belirlemek ve mevzuat düzenlemeleri yapmak, bunların denetimini yapmak ya da yaptırmak, denetimleri yapacak kuruluşların taşımaları gereken nitelikleri belirlemek, bu kuruluşları görevlendirmek, gerektiğinde görevlendirmeyi geçici olarak durdurmak ya da iptal etmek.

Yetkiler

MADDE 6- (1) Başkanlık, görevlerini yerine getirirken aşağıdaki yetkileri kullanır:

a) İlgili mevzuatta yer alan yetkileri kullanmak.

b) Bu Kanun kapsamındakilerin siber saldırılara karşı korunması ve bu saldırıların kaynağına karşı caydırıcılık sağlanması için gerekli tedbiri alır veya aldırır. Bu kapsamda bilişim sistemlerine uygun bulunan yazılım ve donanım ürünlerinin kurulum ve entegrasyonunu sağlayabilir, bu ürünler tarafından üretilen veya toplanan veri ve log kayıtlarını Başkanlık yönetiminde bulunan bilişim sistemlerine aktarabilir, siber olayların tespitine yönelik gerekli yöntemi ve aracı kullanabilir.

c) Bu Kanun kapsamındakilerden siber olaya maruz kalanlara yerinde veya uzaktan siber olay müdahale desteği sağlayabilir, siber uzayda bulunan veya elde ettiği veri, imaj veya log kayıtları üzerinden saldırılara ait izleri takip edebilir, bunları inceleyerek delillendirebilir, suç teşkil ettiği değerlendirilen bulguları adli makamlar ve diğer ilgililer ile paylaşır, yurt içi ve yurt dışındaki paydaşlar ile koordinasyon sağlayabilir.

ç) Bu Kanun kapsamındakilerden, yürüttüğü faaliyetlerle sınırlı olmak üzere bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda elde edilen bilgi, belge, veri ve kayıtlar, en fazla iki yıl süreyle çalışmaya konu edilir ve çalışma süresi sonrasında imha edilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar.

d) Bilişim sistemlerindeki log kayıtlarını bünyesinde toplayabilir, saklayabilir, değerlendirebilir. Bunlar hakkında rapor hazırlayarak ilgili kurum ve kuruluşlar ile paylaşabilir.

e) Başkanlık, bakanlıklar ve diğer kamu kurum ve kuruluşları ile koordineli olarak siber güvenlik konularında ihtiyaç halinde personel tefrik edebilir.

f) Görev alanına giren konularda uluslararası kuruluşlar ve ülkelerle ilişkiler yürütebilir, bilgi alışverişinde bulunabilir, ülkemizi temsil edebilir ve koordinasyonu sağlayabilir, uluslararası kuruluşların çalışmalarına katılabilir, alınan kararların uygulanmasını takip edebilir ve gerekli koordinasyonu sağlayabilir.

g) Bu Kanun kapsamındaki kurum, kuruluş ve ilgili diğer gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşları sınıflandırabilir, faaliyetlerini icra ederken gerektiğinde sadece belirli bir kısmını kapsayan hükümler oluşturabilir.

ğ) Siber güvenlik denetimi gerçekleştiren bağımsız denetçiler ve bağımsız denetim kuruluşlarını yetkilendirebilir, yetkisini süreli veya süresiz iptal edebilir.

h) Kamu kurum ve kuruluşları ile kritik altyapıların bilişim sistemlerinde kullanılacak ve siber güvenliğe etkisi olan yazılım, donanım, ürün ve hizmetlere dair kriterler ile Başkanlığa yapılacak bildirimlere ilişkin usul ve esasları belirler.

ı) Siber güvenlik yazılım, donanım, ürün ve hizmetlerinin asgari güvenlik kriterlerini belirler. Bunları sağlayacak veya tedarik edecek gerçek ve tüzel kişilere yönelik sertifikasyon, yetkilendirme ve belgelendirme süreçlerini yönetir. Siber güvenlik yazılım, donanım, ürün ve hizmetlerinin belirlenecek standartlara uygun hale getirilmesini talep edebilir, bu talebe uyum sağlamayanların kullanılmasını önleyici tedbirler alabilir.

(2) Bu Kanun uyarınca yürütülen iş ve işlemler kapsamında kişisel veriler; hukuka ve dürüstlük kurallarına uygun şekilde, doğru ve gerektiğinde güncel olmak kaydıyla, belirli, açık ve meşru amaçlarla, işlendiği amaçla bağlantılı, sınırlı ve ölçülü olmak kaydıyla ve işlendiği amaç için gerekli olan süre kadar muhafaza edilmek üzere işlenir. Bu Kanunda belirtilen yetkiler çerçevesinde elde edilecek kişisel veriler ve ticari sırlar; bu verilere erişilmesini gerektiren sebeplerin ortadan kalkması halinde resen silinir, yok edilir veya anonim hale getirilir.

(3) Bu maddenin uygulanmasına ilişkin usul ve esaslar Cumhurbaşkanı tarafından çıkarılacak yönetmelikle belirlenir.

Sorumluluklar ve iş birliği

MADDE 7- (1) Bu Kanun kapsamında yer alan ve bilişim sistemleri kullanmak suretiyle hizmet sunan, veri toplayan, işleyen ve benzeri faaliyet yürütenlerin siber güvenliğe ilişkin görev ve sorumlulukları şunlardır:

a) Başkanlığın görev ve faaliyetleri kapsamında talep ettiği her türlü veri, bilgi, belge, donanım, yazılım ve diğer her türlü katkıyı öncelikle ve zamanında Başkanlığa iletmek.

b) Siber güvenliğe yönelik olarak milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almak, hizmet sundukları alanda tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmek.

c) Kamu kurumları 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.

ç) Sertifikasyon, yetkilendirme ve belgelendirmeye tabi siber güvenlik şirketlerince faaliyete başlamadan önce mevcut düzenlemeler çerçevesinde Başkanlığın onayını almak.

d) Siber olgunluğun artırılmasına yönelik Başkanlık tarafından geliştirilen politika, strateji, eylem planı ile yayımlanan diğer düzenleyici işlemlerde yer alan hususları yerine getirmek ve gerekli tedbirleri almak.

(2) Başkanlık, bu Kanunda belirtilen faaliyetlerin yürütülmesinde kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşlarla iş birliği içerisinde çalışır.

Denetim

MADDE 8- (1) Başkanlık, bu Kanunda belirtilen görevleri ile ilgili olarak gerekli gördüğü hallerde Kanunun kapsamına giren her türlü fiil ve işlemi denetleyebilir; bu amaçla mahallinde inceleme yapabilir veya yaptırabilir. Denetim, bu Kanun kapsamındaki kurum, kuruluş ve ilgili diğer gerçek ve tüzel kişilerin bu Kanun hükümleriyle ilgili faaliyet ve işlemlerini kapsar. Denetime Başkanlık personeli, yetkilendirilmiş ve belgelendirilmiş bağımsız denetçiler ve bağımsız denetim kuruluşları yetkilidir. Bu yetki, Başkan tarafından görevlendirilenler tarafından kullanılır. Kamu kurum ve kuruluşları ile kritik altyapılarda denetimler, Başkanlık personelince veya refakatinde yapılır.

(2) Başkanlık, denetim faaliyetlerine ilişkin önemlilik ve öncelik ilkeleri ile risk değerlendirmelerinde dikkate alınacak ölçütleri ve uygulama esaslarını belirler. Denetim faaliyeti, önemlilik ve öncelik

ilkeleri ile risk değerlendirmeleri kapsamında oluşturulacak program uyarınca yürütülür. Başkan, oluşturulan program dışında incelenmesi gerekli görülen hususlarda program dışı denetim yaptırabilir.

(3) Mülki amirler, kolluk kuvvetleri ve diğer kamu kurumlarının amir ve memurları inceleme veya denetimle görevlendirilenlere her türlü kolaylığı göstermek ve yardımda bulunmakla yükümlüdürler.

(4) Denetimle görevlendirilenler; 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 konularında yetkilidir. Denetime tabi tutulanlar, ilgili cihaz, sistem, yazılım ve donanımları verilen sürelerde denetlemeye açık tutmak, denetim için gerekli altyapıyı temin etmek ve çalışır vaziyette tutmak için gerekli önlemleri almak zorundadır.

(5) Millî güvenlik, kamu düzeni, suç işlenmesinin veya siber saldırıların önlenmesi amacıyla hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emri ile konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama yapılabilir, uzun süreli hizmet aksamasına yol açmayacak ve kesintisiz şekilde kopya çıkarma ve el koyma işlemi gerçekleştirilebilir. Çıkarılan kopyanın bir nüshası ilgilisine teslim edilir ve bu husus tutanağa geçirilerek imza altına alınır. Bu işlemlerin yapılabilmesi için makul sebeplerin oluştuğunun gerekçeleriyle birlikte gösterilmesi gerekir. Hâkim kararı olmaksızın yapılan arama ve gerçekleştirilen kopya çıkarma ve el koyma işlemleri yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi hâlde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir ve el koyma kendiliğinden kalkar. Yetkilendirilmiş veri merkezi işletmecilerinin veri merkezlerinde sadece hâkim kararıyla arama, kopya çıkarma ve el koyma işlemi yapılabilir. Bu fıkra kapsamına giren talepler bakımından Ankara sulh ceza hâkimliği yetkili ve görevlidir. Ancak kamu kurum ve kuruluşları bakımından hâkim kararı aranmaz.

Siber Güvenlik Kurulu

MADDE 9- (1) Siber Güvenlik Kurulu; Cumhurbaşkanı, Cumhurbaşkanı Yardımcısı, Adalet Bakanı, Dışişleri Bakanı, İçişleri Bakanı, Milli Savunma Bakanı, Sanayi ve Teknoloji Bakanı, Ulaştırma ve Altyapı Bakanı, Milli Güvenlik Kurulu Genel Sekreteri, Milli İstihbarat Teşkilatı Başkanı, Savunma Sanayii Başkanı ve Siber Güvenlik

Başkanından oluşur. Cumhurbaşkanının katılmadığı hallerde Kurula Cumhurbaşkanı Yardımcısı başkanlık eder.

(2) Kurul toplantılarına üyeler dışında, gündemin özelliğine göre ilgili bakan ve kişiler de çağrılarak bilgi ve görüş alınabilir.

(3) Kurul, görevleri kapsamında gerekli görmesi halinde komisyon ve çalışma grupları oluşturabilir. Komisyon ve çalışma grupları, Kurulun görev alanına giren hususlarda teknik düzeyde çalışmalar yapar ve karar önerileri oluşturur. Komisyon ve çalışma grubu toplantılarına görüşlerinden faydalanmak üzere alanında uzman kişiler davet edilebilir.

(4) Kurulun görevleri şunlardır:

a) Siber güvenlikle ilgili politika, strateji, eylem planı ve diğer düzenleyici işlemlere yönelik kararları almak, alınan kararların tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.

b) Başkanlık tarafından hazırlanan siber güvenlik alanına ilişkin teknoloji yol haritasının ülke çapında uygulanmasına yönelik kararlar almak.

c) Siber güvenlik alanında teşvik verilecek öncelikli alanları belirlemek, siber güvenlik alanındaki insan kaynağının geliştirilmesine yönelik karar almak.

ç) Kritik altyapı sektörlerini belirlemek.

d) Başkanlık ile kamu kurum ve kuruluşları arasında meydana gelebilecek ihtilaflar hakkında karar almak.

(5) Kurulun sekretarya hizmetleri Başkanlık tarafından yürütülür. Kurul, komisyon ve çalışma gruplarının çalışma usul ve esasları Cumhurbaşkanı tarafından çıkarılacak yönetmelikle belirlenir.

ÜÇÜNCÜ BÖLÜM
Personele İlişkin Hükümler

Sözleşmeli uzman personel istihdamı

MADDE 10- (1) Başkanlıkta siber güvenliğin sağlanması ile ilgili görevleri yürütmek üzere sayısı Cumhurbaşkanınca belirlenecek sözleşmeli uzman personel çalıştırılabilir. Bu personelin nitelikleri, atanma şartları gibi istihdamlarına ilişkin hususlar ile bunlara verilecek her türlü ödemeler dahil net ücretler, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 4 üncü maddesinin (B) bendine göre çalıştırılanlar için uygulanmakta olan sözleşme ücret tavanının beş katını aşmamak üzere

Siber Güvenlik Kurulu tarafından ilgililerin yürüteceği görevler göz önüne alınarak tespit edilir. Bu fıkra kapsamındaki personel, 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında sigortalı sayılır. Kanunlardaki özel hükümler saklı kalmak kaydıyla, bu statüde çalıştırılma, sözleşme bitiminde kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmez.

(2) Başkanlıkta; geçici olarak görevlendirilenler de dahil olmak üzere, görev alan tüm personele 7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu uyarınca güvenlik soruşturması ve arşiv araştırması birlikte yapılır.

Zorunlu hizmet yükümlülüklerinin devri

MADDE 11- (1) Başkanlıkta istihdam edilen personelden ilgili mevzuatı kapsamında diğer kamu kurum ve kuruluşlarına karşı zorunlu hizmet yükümlülüğü bulunanların Başkanlıkta geçen hizmet süreleri, ilgili kamu kurum ve kuruluşunun da muvafakati alınmak kaydıyla, söz konusu yükümlülük sürelerinden düşülür.

Yasak hükümler

MADDE 12- (1) Başkanlıkta kadrolu veya sözleşmeli statüde görev yapanlardan Başkanlık ile herhangi bir nedenle ilişiği kesilenler Başkanlıktan muvafakat almadan iki yıl süreyle yurt içi veya yurt dışında siber güvenlik alanında resmi veya özel başka hiçbir görev alamaz ve bu alanda ticaretle uğraşamaz, serbest meslek faaliyetinde bulunamaz ve özellikle bu sektörde faaliyet gösteren bir şirkette hissedar veya yönetici olamaz.

(2) Başkanlıktaki görev ve faaliyetler kapsamında edinilen bilgi, belge ve benzeri her türlü verinin, Başkanlıkça yetki verilen durumlar hariç olmak üzere, radyo, televizyon, internet, sosyal medya, gazete, dergi, kitap ve diğer tüm medya araçları ile her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim araçları vasıtasıyla yayımlanması veya açıklanması yasaktır.

Sır saklama yükümlülüğü

MADDE 13- (1) 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.

DÖRDÜNCÜ BÖLÜM
Gelir ve Muafiyetler

Başkanlığın gelirleri

MADDE 14- (1) Başkanlığın gelirleri;

a) Genel bütçeden yapılacak Hazine yardımlarından,

b) Başkanlığın faaliyetlerinden elde edilen gelirlerden,

c) Başkanlık tarafından verilen idari para cezalarından elde edilen gelirlerden,

ç) Kanun ve kararnamelerle kurulu bulunan ve kurulacak olan fonların gelirlerinden Cumhurbaşkanı kararıyla yüzde 10'una kadar aktarılacak tutarlardan,

d) Diğer gelirlerden,

oluşur.

Muafiyetler

MADDE 15- (1) Başkanlığın ihtiyaçları kapsamında yurt dışından ithalat veya hibe yoluyla sağlanacak her türlü malzeme, araç, gereç, makine, cihaz ve sistemleri ve bunların araştırma, geliştirme, eğitim, üretim, modernizasyon ve yazılımı ile yapım, bakım ve onarımlarında kullanılacak yedek parçalar, hammadde malzeme ile bedelsiz olarak dış kaynaklardan alınan yardım malzemeleri nedeniyle yapılacak işlemler gümrük vergisinden, fon ve resimlerden, harçlardan, bu işlemler nedeniyle düzenlenen kâğıtlar damga vergisinden istisnadır. Bu istisna, Başkanlık adına yurt dışına onarım, modernizasyon, bakım, mahrece iade, değişim maksadıyla kati çıkış, geçici çıkış, bedelsiz ithalat ve giriş işlemlerinde de uygulanır.

(2) Başkanlığın görevlerinin yürütülmesi sırasında ihtiyaç duyduğu her türlü malzeme, araç, gereç, makine, cihaz ve sistemlerin ithalatında ve yurt dışına çıkış aşamalarında, kamu kurum ve kuruluşlarından, gerçek ve tüzel kişilerden alınması gereken izin ve uygunluk belgesi aranmaz.

(3) Kamu kurum ve kuruluşları ile diğer kurum ve kuruluşlar, bu Kanunda yazılı görevlerin yerine getirilmesi sırasında ihtiyaç duyulan hâllerde, kullanımlarında bulunan ve müsadere edilen her türlü malzeme, ekipman, teçhizat ve cihazı, diğer kanunların bu konudaki düzenlemelerine bakılmaksızın Başkanlığa geçici olarak tahsis edebilir veya bedelsiz devredebilirler.

BEŞİNCİ BÖLÜM

Cezai Hükümler ve İdari Para Cezalarının Uygulanması

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) Bu Kanun uyarınca alınması gerekli onay, yetki veya izinleri almaksızın faaliyet yürütenler iki yıldan dört yıla kadar hapis ve bin günden ikibin güne kadar adli para cezası ile cezalandırılır.

(3) Sır saklama yükümlülüğünü yerine getirmeyenlere dört yıldan sekiz yıla kadar hapis cezası verilir.

(4) Siber uzayda veri sızıntısı nedeniyle daha önce yer alan kişisel veya kritik kamu hizmeti kapsamına giren kurumsal verileri, kişilerin veya kurumların izni olmaksızın ücretli veya ücretsiz şekilde erişime açan, paylaşan veya satışa çıkaranlara üç yıldan beş yıla kadar hapis cezası verilir.

(5) Siber uzayda veri sızıntısı olmadığını bildiği halde 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 oluşturanlara veya bu maksatla bu içerikleri yayanlara iki yıldan beş yıla kadar hapis cezası verilir.

(6) Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren unsurlarına yönelik olarak siber saldırıda bulunan veya bu saldırı neticesinde elde ettiği her türlü veriyi siber uzayda bulunduranlara fiil daha ağır bir cezayı gerektiren başka bir suç oluşturmadığı takdirde sekiz yıldan oniki yıla kadar hapis cezası verilir. Bu saldırı neticesinde elde ettiği her türlü veriyi siber uzayda yayan, başka bir yere gönderen veya satışa çıkaranlara on yıldan onbeş yıla kadar hapis cezası verilir.

(7) Yukarıdaki fıkralara göre verilecek ceza 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 iki katına kadar artırılır.

(8) 12 nci maddeye aykırı davrananlara üç yıldan beş yıla kadar hapis cezası verilir.

(9) Bu Kanundan kaynaklanan görev ve yetkilerini kötüye kullananlara veya kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket etmek suretiyle veri ihlali yaşanmasına sebebiyet verenlere bir yıldan üç yıla kadar hapis cezası verilir.

(10) 7 nci maddenin birinci fıkrasının (b) ve (c) bentlerindeki görev ve sorumluluklarını yerine getirmeyenlere bir milyon Türk lirasından on milyon Türk lirasına kadar, 18 inci maddedeki görev ve sorumluluklarını yerine getirmeyenlere ise on milyon Türk lirasından yüz milyon Türk lirasına kadar idari para cezası verilir.

(11) 8 inci maddenin dördüncü fıkrasındaki yükümlülüklerini yerine getirmeyenlere, yüzbin Türk lirasından bir milyon Türk lirasına kadar, bu yükümlülüklerin ticari şirketlerce yerine getirilmemesi halinde yüzbin Türk lirasından az olmamak üzere bağımsız denetimden geçmiş yıllık finansal tablolarında yer alan brüt satış hasılatının yüzde 5'ine kadar idari para cezası verilir.

İdari para cezalarının uygulanması

MADDE 17- (1) İdari para cezalarının uygulanmasından önce ilgilinin savunması alınır. Savunma istendiğine ilişkin yazının tebliğ tarihinden itibaren otuz gün içinde savunma verilmemesi halinde, ilgilinin savunma hakkından feragat ettiği kabul edilir.

(2) Bu Kanunda tanımlanan kabahatlerden birinin idari yaptırım kararı verilinceye kadar birden çok işlendiğinin tespit edilmesi halinde ilgili gerçek veya tüzel kişiye tek idari para cezası verilir ve verilecek ceza iki katını aşmayacak şekilde artırılarak uygulanır. Kabahatin işlenmesi nedeniyle bir menfaat temin edilmesi veya zarara sebebiyet verilmesi halinde verilecek idari para cezasının miktarı bu menfaat veya zararın üç katından az beş katından fazla olamaz.

(3) Başkanlık tarafından verilen idari para cezaları, tebliğ tarihinden itibaren bir ay içinde ödenir. Bu süre içinde ödenmeyen ve kesinleşen idari para cezaları, Kurumun bildirimi üzerine 21/7/1953 tarihli ve 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre vergi dairelerince tahsil edilir.

(4) Tahsil edilen idari para cezalarının yüzde ellisi Başkanlık bütçesine, yüzde ellisi genel bütçeye gelir kaydedilir. Başkanlığın tahsil ettiği idari para cezalarından ayrılan genel bütçe payı; vergi dairesince tahsil edilen idari para cezalarından ayrılan Başkanlık payı, tahsilatı takip eden ay sonuna kadar aktarılır.

(5) Bu Kanun uyarınca verilen idari para cezası kararlarına karşı idari yargı yoluna başvurulabilir.

ALTINCI BÖLÜM
Çeşitli ve Son Hükümler

Siber güvenlik ürünleri ve şirketleri

MADDE 18- (1) Siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerin yurt dışına satışı, Başkanlıkça belirlenecek usul ve esaslara uygun olarak yapılır. Bu usul ve esaslarda yer alacak izne tabi ürünlerin yurt dışına satışında Başkanlık onayı alınır.

(2) Siber güvenlik ürün, sistem, yazılım, donanım ve hizmetleri üreten şirketlerin birleşme, bölünme, pay devri veya satış işlemleri Başkanlığa bildirilir. Bu işlemler kapsamında gerçek veya tüzel kişilere münferiden veya birlikte şirket üzerinde doğrudan veya dolaylı kontrol hakkı veya karar alma yetkisi sağlayan işlemler Başkanlık onayına tabidir.

(3) Başkanlık onayı alınmaksızın gerçekleştirilen işlemler hukuki bir geçerlilik kazanmaz. Başkanlık, bu madde kapsamında yapılacak işlemlerle ilgili olarak kurum ve kuruluşlardan bilgi ve belge talep edebilir.

(4) Bu maddenin uygulanmasına ilişkin hususlar Başkanlık tarafından yayımlanacak usul ve esaslar ile belirlenir.

Değiştirilen ve yürürlükten kaldırılan hükümler

MADDE 19- (1) 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararnamenin ek 34 üncü maddesinin üçüncü fıkrasına aşağıdaki cümle eklenmiştir.

“Siber Güvenlik Başkanı, mali ve sosyal hak ve yardımlar ile emeklilik hakları bakımından, bu fıkrada belirtilen usul ve esaslar çerçevesinde bakanlık müsteşarına denk kabul edilir.”

(2) 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa ekli (II) sayılı Cetvelin “B) Özel Bütçeli Diğer İdareler” bölümüne aşağıdaki satır eklenmiştir.

“46) Siber Güvenlik Başkanlığı”

(3) 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 10 uncu maddesinin altıncı fıkrası aşağıdaki şekilde değiştirilmiştir.

“(6) Kurum, görevleri kapsamında, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin

aldırılması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar.”

(4) 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun;

a) 5 inci maddesinin birinci fıkrasının (h) bendi yürürlükten kaldırılmış ve (ı) bendi aşağıdaki şekilde değiştirilmiştir.

“ı) Bakanlığın yürüttüğü görevler kapsamındaki veri ve sistemlerin barındırılacağı veri merkezleri ve verilerin transferi için gerekli altyapıları kurmak, kurdurmak, işletmek, işlettirmek, bu merkezlere yönelik politika, strateji ve hedefleri belirlemek, eylem planlarını hazırlamak, eylem planlarını izlemek ve tüm bu faaliyetlere yönelik uygulama usul ve esaslarını belirlemek, kurulum, uygulama ve işletim süreçlerini planlamak, yürütmek ve koordine etmek.”

b) 6 ncı maddesinin birinci fıkrasının (v) bendi aşağıdaki şekilde değiştirilmiştir.

“v) İnternet alan adları ve Kurum görevleri konularında Cumhurbaşkanı ve Bakanlık tarafından verilen görevleri yerine getirmek.”

c) 60 ıncı maddesinin onbirinci fıkrası ile ek 1 inci ve ek 2 nci maddeleri yürürlükten kaldırılmıştır.

Uyum, geçiş düzenlemeleri ve kuruluş işlemleri

GEÇİCİ MADDE 1- (1) Bilgi Teknolojileri ve İletişim Kurumu Başkanlığına ve Dijital Dönüşüm Ofisine ait ve münhasıran ulusal siber güvenlik faaliyetleri kapsamında kullanılan her türlü taşınır, bilgi işlem altyapısı ve sistemler, taşıt, araç, gereç ve malzeme, fiziki ve elektronik ortamdaki her türlü kayıt ve doküman ile diğer her türlü varlık envanteri ile mezkûr Başkanlık ve Ofis tarafından söz konusu faaliyetlerin yürütülmesinden doğan her türlü borç ve alacaklar, hak ve yükümlülükler, Siber Güvenlik Başkanlığına bu Kanunun yayımından itibaren altı ay içerisinde devredilir.

(2) Bilgi Teknolojileri ve İletişim Kurumu Başkanlığının ve Dijital Dönüşüm Ofisinin kadro ve pozisyonlarında bulunan personelden ulusal siber güvenlik faaliyetleri kapsamında çalışanlar, taleplerinin bulunması ve Siber Güvenlik Başkanlığınca uygun görülmesi halinde Başkanlıkta görevlendirilebilirler. Bunlardan talepte bulunan ve Başkanlıkça uygun görülenler mevcut kadro veya pozisyon unvanları ve öğrenim durumları dikkate alınarak bu Kanunun yayımından itibaren dokuz ay içerisinde Başkanlıkta durumlarına uygun kadro veya pozisyonlara atanabilirler. Bu fıkra kapsamında ataması yapılan personelin önceki kurumlarında veya

kadrolarında geçirdikleri süreler yeni kurumlarında veya kadrolarında geçirilmiş sayılır. Bu fıkra kapsamında ataması yapılan personelden mali hakları hususunda haklarında 375 sayılı Kanun Hükmünde Kararnamenin geçici 10 uncu maddesi veya ilgili diğer mevzuat hükümleri uygulananlar hakkında anılan düzenlemelerin uygulanmasına devam edilir. Dijital Dönüşüm Ofisinden bu fıkra kapsamında ataması yapılan personele, iş mevzuatına göre herhangi bir tazminat ve yıllık izin ücreti ödenmez. Bu personelin önceden kıdem tazminatı ödenmiş süreleri hariç kıdem tazminatına hak kazanacak şekilde geçmiş olan hizmet süreleri, ilgisine göre emekli ikramiyelerinin veya iş sonu tazminatının hesabında dikkate alınır. Ayrıca, bu personele bu fıkraya göre atanmadan önce ilave tediye veya ikramiye ödenmiş olması halinde ödenen tutarların atamanın yapıldığı tarihten sonraki çalışılmayan günlere tekabül eden kısmı geri alınır.

(3) Bilgi Teknolojileri ve İletişim Kurumu Başkanlığının ve Dijital Dönüşüm Ofisinin ulusal siber güvenlik faaliyetleri ile ilgili yapılmış olan sözleşmeler, açılmış ve açılacak olan davalar ve icra işlemlerinde ikinci fıkradaki atama işlemlerinin tamamlanması tarihi itibarıyla Başkanlık taraf sıfatını kazanır, mevcut dava dosyaları ve icra takiplerine ilişkin dosyalar Başkanlığa devredilir.

(4) Siber güvenlik alanında faaliyet icra eden dernek, derneklerden oluşan federasyonlar, vakıflar ile ticaret şirketleri, altıncı fıkrada belirtilen düzenlemelerin yürürlüğe girmesinden itibaren bir yıl içerisinde Başkanlığın belirlediği ilke ve esaslar çerçevesinde sertifikasyon, yetkilendirme ve belgelendirme işlemlerini tamamlamakla yükümlüdürler. Bu yükümlülüğün yerine getirilmemesi halinde siber güvenlik alanında faaliyette bulunulamaz. Bu süre sonunda söz konusu yükümlülüklerini yerine getirmeyen dernek, vakıf ve federasyonların tüzel kişiliklerine, Başkanlığın talebi üzerine 22/11/2001 tarihli ve 4721 sayılı Türk Medenî Kanununun ilgili hükümlerine göre mahkeme kararıyla son verilir ve mahkeme tarafından yargılama sürecinde gerekli tedbirler alınır. Ticaret şirketleri ise aynı süre içinde yükümlülüklerini yerine getirmediği takdirde ticaret unvanlarında ve faaliyet konularında yer alan siber güvenliğe ilişkin ibareleri şirket sözleşmelerinden çıkarır veya ticaret sicilinden terkin edilmeleri amacıyla tasfiye süreçlerini başlatır.

(5) 19 uncu maddenin üçüncü ve dördüncü fıkraları uyarınca yürürlükten kaldırılan hükümler kapsamında faaliyet gösteren kurumlar Başkanlığın teşkilatlanmasının tamamlanmasına kadar anılan hükümler çerçevesinde görevlerini yürütmeye devam ederler.

(6) Bu Kanunun uygulanmasına ilişkin düzenlemeler, bir yıl içinde yürürlüğe konulur. Bu düzenlemeler yürürlüğe girinceye kadar mevcut düzenlemelerin bu Kanuna aykırı olmayan hükümlerinin uygulanmasına devam olunur.

Yürürlük

MADDE 20- (1) Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 21- (1) Bu Kanun hükümlerini Cumhurbaşkanı yürütür.