TÜRKİYE BÜYÜK MİLLET MECLİSİ

YASAMA DÖNEMİ	YASAMA YILI
28	3

SIRA SAYISI: 190

Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Siber Güvenlik Kanunu Teklifi (2/2860) ve Milli Savunma Komisyonu Raporu

Not: Bu Sıra Sayısına; elektronik ortamda
https://www.tbmm.gov.tr/yasama/komisyon-raporlari
internet adresindeki sorgu sayfası üzerinden erişilebilmektedir.

Kanunlar ve Kararlar Başkanlığı

İÇİNDEKİLER

Sayfa

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Siber Güvenlik Kanunu Teklifimiz ve gerekçesi ekte sunulmaktadır.

Gereğini arz ederiz.

Ali Özkaya Afyonkarahisar	*Atay Uslu* Antalya	*Tuğba Işık Ercan* İstanbul
Mahmut Rıdvan Nazırlı Elâzığ	*Orhan Kırcalı* Samsun	*Mehmet Uğur Gökgöz* Isparta
Yusuf Ziya Aldatmaz Bartın	*Asuman Erdoğan* Ankara	*Tamer Akkal* Manisa
Saffet Bozkurt Zonguldak	*Erol Keleş* Elâzığ	*Murat Baybatur* Manisa
Hüseyin Özhan Adıyaman	*Arslan Tatar* Şırnak	*Zeki Korkutata* Bingöl
İrfan Çelikaslan Gaziantep	*Lütfi Bayraktar* Sakarya	*Resul Kurt* Adıyaman
Cevahir Asuman Yazmacı Şanlıurfa	*Abdürrahim Dusak* Şanlıurfa	*Ejder Açıkkapı* Elâzığ
Çiğdem Koncagül Tekirdağ	*Seydi Gülsoy* Osmaniye	*Murat Cahid Cıngı* Kayseri
Nazım Maviş Sinop	*Bülent Tüfenkci* Malatya	*Tahir Akyürek* Konya
Ercan Öztürk Düzce	*Mehmet Demir* Kütahya	*Yüksel Coşkunyürek* Bolu
Ertuğrul Kocacık Sakarya	*Meliha Akyol* Yalova	*Adem Çalkın* Kars
Emel Gözükara Durmaz Bursa	*Seda Gören Bölük* İstanbul	*Cüneyt Yüksel* İstanbul
Veysal Tipioğlu Kocaeli	*Mervan Gül* Siirt	*Yılmaz Büyükaydın* Trabzon
Kadem Mete Muğla	*Hasan Çilez* Amasya	*Ömer Oruç Bilal Debgici* Kahramanmaraş

Halit Yerebakan İstanbul	*Hüseyin Altınsoy* Aksaray	*Cahit Özkan* Denizli
Cevahir Uzkurt Niğde	*Adem Korkmaz* Burdur	*Mehmet Emin Öz* Erzurum
İsmail Güneş Uşak	*Süleyman Özgün* Nevşehir	*Şaban Çopuroğlu* Kayseri
Mehmet Şahin Kahramanmaraş	*Kayhan Türkmenoğlu* Van	*Mesut Bozatlı* Gaziantep
Bünyamin Bozgeyik Gaziantep	*Lütfiye Selva Çam* Ankara	*Fatma Serap Ekmekci* Kastamonu
Radiye Sezer Katırcıoğlu Kocaeli	*Fatma Aksal* Edirne	*Refik Özen* Bursa
Ümmügülşen Öztürk İstanbul	*Fatma Öncü* Erzurum	*Kaan Koç* Ardahan
Hakan Aksu Sivas	*Adem Yeşildal* Hatay	*Kemal Karahan* Hatay
Yakup Otgöz Muğla	*Celalettin Köse* Gümüşhane	*İbrahim Ethem Taş* Antalya
Yusuf Ahlatcı Çorum	*Seda Sarıbaş* Aydın	*Mehmet Baykan* Konya
Mustafa Yavuz Bursa	*Ömer İleri* Ankara	*Abdullah Doğru* Adana
Muammer Avcı Zonguldak	*Faruk Aytek* Adana	*Ziya Altunyaldız* Konya
Mustafa Alkayış Adıyaman	*Ruken Kilerci* Ağrı	*Orhan Yegin* Ankara
Şengül Karslı İstanbul	*Mustafa Demir* İstanbul	*Mustafa Canbey* Balıkesir
Ahmet Mücahit Arınç Manisa	*Mestan Özcan* Tekirdağ	*İbrahim Yurdunuseven* Afyonkarahisar
Necmettin Erkan Kırşehir	*Osman Sağlam* Karaman	*Emre Çalışkan* Nevşehir

Derya Ayaydın
İstanbul

Süleyman Şahan
Yozgat

Hüseyin Yayman
Hatay

Hulusi Akar
Kayseri

Adil Biçer
Kütahya

Harun Mertoğlu
Rize

Ali İnci
Sakarya

Büşra Paker
İstanbul

Ayhan Salman
Bursa

Mevlüt Kurt
Kahramanmaraş

Faruk Kılıç
Mardin

Mustafa Kaplan
Kırıkkale

Selman Özboyacı
Konya

Hasan Turan
İstanbul

Sayın Bayar Özsoy
Kayseri

Rümeysa Kadak
İstanbul

Mehmet Sait Yaz
Diyarbakır

Fuat Oktay
Ankara

Suat Pamukçu
İstanbul

Latif Selvi
Konya

Rukiye Toy
Sivas

Mehmet Eyup Özkeçeci
Gaziantep

Hasan Arslan
Afyonkarahisar

İbrahim Eyyüpoğlu
Şanlıurfa

Mustafa Oğuz
Burdur

Cüneyt Aldemir
Tokat

Nurettin Alan
İstanbul

Osman Zabun
Isparta

İnanç Siraç Kara Ölmeztoprak
Malatya

Jülide Sarıeroğlu
Ankara

Yahya Çelik
İstanbul

Fehmi Alpay Özalan
İzmir

Şahin Tin
Denizli

Ahmet Fethan Baykoç
Ankara

Mustafa Hakan Özer
Konya

Zehranur Aydemir
Ankara

Yücel Arzen Hacıoğulları
İstanbul

İsmail Erdem
İstanbul

Abdurrahim Fırat
Erzurum

Mustafa Arslan
Tokat

Ali Kıratlı
Mersin

Ali Temür
Giresun

Ersan Aksu
Samsun

KATILMA YAZILARI

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

10/01/2025 tarihinde sunulan 2/2860 Esas Numaralı Siber Güvenlik Kanunu Teklifi'ne imzamı eklemek ister, gereğini bilgilerinize arz ederim.

Zeynep Yıldız
Ankara

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

2/2860 Esas Numaralı Siber Güvenlik Kanunu Teklifi'ne katılıyorum. Gereğini arz ederim.

13/01/2025
Nazım Elmas
Giresun

HAVALE EDİLDİĞİ KOMİSYONLAR (2/2860)	
ESAS	Milli Savunma Komisyonu
TALİ	Adalet Komisyonu Plan ve Bütçe Komisyonu Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonu

GENEL GEREKÇE

Günümüzde siber güvenlik, dijitalleşmenin hız kazandığı bir dünyada kritik önceliklerden biri haline gelmiştir. Hem bireylerin hem de kurumların dijital varlıklarını koruma ihtiyacı, gelişmiş ülkelerde stratejik öneme sahip olan siber güvenlik politikalarını ve teknolojik yatırımları beraberinde getirmiştir. Yapay zekâ, blok zincir, büyük veri, kuantum ve bulut bilişim gibi teknolojilerin yaygınlaşması, siber tehditlerin karmaşıklığını artırırken, aynı zamanda savunma mekanizmalarının gelişimini de tetiklemiştir. Kritik altyapıların korunması ve kamu kurumlarının dijital süreç ve varlıklarının güvence altına alınması, modern siber güvenlik stratejilerinin merkezinde yer almaktadır. Bununla beraber, Milli Teknoloji Hamlesi kapsamında ülkemizin yaşadığı teknolojik dönüşüm ve gelişim sürecinde siber güvenlik en temel gerekliliklerinden biri haline gelmiştir.

Ülkemizin özellikle son 20 yılda teknolojide yaptığı atılım internet kullanıcı sayısını da artırmıştır. Araştırmalara göre, ülkemizde internet kullanıcıları günlük ortalama 7,5 saat internette zaman geçirmekte ve bunun yaklaşık 3 saatini sosyal medya üzerinde harcamaktadır. Mobil abone sayısı 93,3 milyona, mobil genişbant abone sayısı 72,7 milyona ve sabit genişbant kullanıcıları yaklaşık 19,9 milyona ulaşmıştır. Mobil internet kullanıcılarının ortalama aylık veri tüketimi 16,7 GB iken, sabit genişbant abonelerinin aylık ortalama kullanımı 272 GB olarak ölçülmüştür. Bu veriler, ülkemizin iletişim altyapısındaki hızlı gelişimi ve dijitalleşmenin günlük hayattaki etkisini açıkça ortaya koymaktadır.

Diğer taraftan, bağlı cihaz sayısının ve akıllı uygulamaların artmasıyla tüm dünyada üretilen veri miktarında ciddi bir artış yaşanmaktadır. Üretilen verinin 2024 itibarıyla 180 zettabayt sınırlarına ulaşması, veri işlemeye dayalı hizmetler ile çözümlerin gerek iş hayatında gerekse gündelik yaşamda önemli bir yer tutmasına yol açmıştır. 2004 yılında üretilen toplam veri miktarının yalnızca 5 exabayt civarında olduğu göz önüne alındığında, geçen süre zarfında üretilen veri miktarının yaklaşık 36 bin kat arttığı görülmektedir. Bu artış, dijitalleşmenin hızını ve veri odaklı teknolojilerin hayatımızdaki etkisini çarpıcı bir şekilde ortaya koymaktadır.

Konvansiyonel savaşlar yerini hibrit ve asimetrik savaşlara bırakmış, devlet destekli siber saldırılar başta olmak üzere terör örgütleri, organize suç örgütleri ve bireysel motivasyonla hareket eden siber tehdit aktörleri tarafından devlet kurumları, enerji, finans, sağlık ve haberleşme sistemleri gibi kritik altyapılar ile her türlü teknolojik cihaz hedef alınmaya başlanmıştır. Siber saldırıların devlet politikalarının bir aracı olarak kullanılmasındaki artış, savaş ve barış halleri arasındaki sınırı belirsizleştirmiş, ülkeler direkt askeri misillemeden kaçınmak için siber saldırıları; siyasi, ekonomik ve askeri hedeflere yönelik düşük maliyetli yüksek etkili bir strateji haline getirmiştir. Ayrıca tedarik zincirlerine yönelik saldırılar sonucunda, birçok sektörde kritik sistemler çökmüş ve kesintiler yaşanmıştır.

2024 yılı itibarıyla siber saldırılar, küresel ölçekte her gün yoğunlaşarak karmaşık bir tehdit oluşturmaya devam etmiştir. Üçüncü çeyrekte, her bir kuruluş başına haftalık ortalama 1.876 siber saldırı gerçekleştirilmiş, bu da 2023'ün aynı dönemine göre %75'lik bir artışı ifade etmektedir.

Bir ülkenin siber güvenlik alanında ön plana çıkarak rol model olabilmesi, kapsamlı bir siber güvenlik çatı mevzuatının varlığı ve merkezi bir otoritenin etkin işleyişiyle doğrudan ilişkilidir. Çatı bir mevzuat, ulusal düzeyde siber güvenlik politikalarının tutarlılığını sağlamanın yanı sıra kamu kurumları, özel sektör ve bireyler için bağlayıcı standartlar sunmaktadır. Ayrıca, uluslararası iş birliği ve karşılıklı tanınabilirlik açısından temel bir çerçeve sağlayarak, bir ülkenin küresel siber güvenlik ekosistemindeki konumunu güçlendirmektedir. Bu mevzuatın etkili bir şekilde uygulanması, merkezi bir otoritenin varlığıyla mümkün hale gelmektedir. Çünkü, merkezi bir yapı, kaynakların verimli kullanımını, hızlı ve koordineli karar alma mekanizmalarını desteklemekte ve aynı zamanda, tehditlerin daha etkili tespit edilmesi, müdahale süreçlerinin uyum içinde yürütülmesi ve stratejik hedeflere odaklanılması için bir temel oluşturmaktadır.

2024 yılında Uluslararası Telekomünikasyon Birliği tarafından yayımlanan Küresel Siber Güvenlik Endeksi verilerine göre "Rol Model Ülke" kategorisi içerisinde yer alan 46 ülkenin siber güvenlik yapısı ve mevzuatı incelendiğinde; bu ülkelerin yaklaşık %91'i, kapsamlı bir çatı mevzuata sahip olup kişisel verilerin korunması, siber suçların önlenmesi ve kritik altyapıların güvenliği gibi konularda net bir hukuki çerçeve sunmaktadır. Ancak ülkemiz, "Rol Model Ülke" kategorisinde yer almasına rağmen gerçek anlamda çatı mevzuat özelliği teşkil edecek kapsamlı bir siber güvenlik kanununa sahip değildir. Ülkemizdeki siber güvenlik yapılanmasında Ulaştırma ve Altyapı Bakanlığı, Sanayi ve Teknoloji Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi başta olmak üzere birçok kamu kurumunun sorumlulukları bulunmaktadır. Ayrıca çatı mevzuat eksikliği; veri güvenliği, ekosistem iş birlikleri, mevzuat düzenlemeleri, teşvik ve

destekleri yönlendirme, uluslararası iş birlikleri, makro politika oluşturma ve benzeri birçok açıdan koordinasyon problemleri oluşturmaktadır. Çatı mevzuatın oluşturulması ülkemizin küresel endekslerde üst sıralara yükselmesine katkı sağlayacaktır.

Tüm bu hususlar; ülkemizde halen farklı yapılar altında sürdürülmeye çalışılan siber güvenlik yaklaşımının, yeniden yapılandırılması ihtiyacını ortaya koymaktadır.

Bu kapsamda Teklifle;

- Ülkemizin siber güvenlikle ilgili politika ve stratejisini belirlemek üzere Siber Güvenlik Kurulunun kurulması,
- Siber güvenlik alanında geliştirilen politikaların ulusal satıhta etkin bir şekilde uygulanması,
- Kamu kurumları ile kritik altyapı kuruluşlarının siber mukavemetinin ve siber olgunluk seviyesinin artırılması,
- Güncel teknolojik gelişmelerin takip edilmesi ve siber güvenlik süreçlerine entegre edilmesi,
- Kamu kurumları ve kritik altyapı kuruluşlarının bilişim sistemlerinde oluşabilecek siber güvenlik olaylarının merkezi bir bakış açısıyla izlenmesi, tespiti ve bertaraf edilmesi,
- Eylem planlarının ve ikincil mevzuatların hayata geçirilmesi,
- Denetim ve özellikle caydırıcı yaptırım süreçlerinin işletilmesi,
- Siber güvenlik ekosisteminin güçlendirilmesi,
- Standardizasyon, sertifikasyon ve yetkilendirme süreçlerinin düzenlenmesi,
- Siber suçlara yönelik cezaların artırılması suretiyle caydırıcılığın sağlanması amaçlanmaktadır.

MADDE GEREKÇELERİ

Madde 1- Madde ile ülkemizin siber saldırılara karşı korunmasına yönelik gerekli düzenlemelerin yapılması, siber güvenliğinin güçlendirilmesi için strateji ve politikaların belirlenmesi ve Siber Güvenlik Kurulu ihdas edilmesi öngörülmektedir.

Madde 2- Madde ile Kanunun kapsamına ilişkin genel çerçevenin belirlenmesi amaçlanmakta, milli güvenlik istihbaratını Devlet çapında oluşturmakla görevli Milli İstihbarat Teşkilatının yürüttüğü faaliyetleri ile Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının yürüttükleri istihbari nitelikteki faaliyetler kanun kapsamı dışında tutulmaktadır.

Madde 3- Madde ile Kanunda yer alan tanım ve kısaltmaların açıklamalarına yer verilmektedir.

Madde 4- Madde ile siber güvenlik için temel alınan; kurumsallık, süreklilik, sürdürülebilirlik, hesap verilebilirlik, hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması gibi ilkelere yer verilmektedir.

Madde 5- Madde ile Siber Güvenlik Başkanlığının; Cumhurbaşkanlığı Kararnamesi ile belirlenen görevlerinin yanı sıra; kritik altyapı ve bilişim sistemlerinin siber dayanıklılığını artırmak, bunları siber saldırılara karşı korumak, sertifikasyon, yetkilendirme ve belgelendirme faaliyetleri yürütmek, siber mukavemeti artırmak, siber güvenlik alanında faaliyet gösterenlerin uyması gereken usul ve esasları belirlemek gibi görevleri düzenlenmekte ve KamuNet kamu sanal ağ altyapısının ve ulusal kamu entegre veri merkezlerinin kurulmasına ilişkin görevler Başkanlığa devredilmektedir.

Madde 6- Madde ile Siber Güvenlik Başkanlığının görevlerini yerine getirmesi esnasında, Cumhurbaşkanlığı Kararnamesi ile belirlenen yetkilerinin yanı sıra kullanacağı; kamu kurumları ve kritik altyapı kuruluşlarından veri ve log kayıtlarını kendi yönetiminde bulunan bilişim sistemlerine aktarabilme, yürüttüğü faaliyetlerle sınırlı olmak kaydıyla ilgili kurum, kuruluş ve şahıslardan gerekli

bilgi, belge, veri ve kayıtları alabilme, siber güvenlik denetim faaliyetlerini yürütme gibi yetkilerine ilişkin düzenleme yapılmaktadır.

Madde 7- Madde ile bilişim sistemleri kullanmak suretiyle hizmet sunan, veri toplayan, işleyen ve benzeri faaliyet yürütenlerin, siber güvenliğe ilişkin görev ve sorumluluklarının belirlenmesi sağlanmaktadır.

Madde 8- Madde ile siber güvenlik alanında Başkanlık tarafından gerçekleştirilecek rutin veya olay üzerine denetim faaliyetine ilişkin esaslar ile mahallinde yapılacak incelemelere yönelik hususlar belirlenmektedir.

Madde 9- Madde ile siber güvenlikle ilgili politika, strateji, eylem planı ve diğer düzenleyici işlemlere yönelik kararları almak üzere Siber Güvenlik Kurulu oluşturulmakta ve Kurulun kimlerden oluşacağı düzenlenmektedir.

Madde 10- Madde ile Başkanlıkta sözleşmeli uzman personel istihdam yöntemi ile ücretlerine ilişkin esaslar belirlenmektedir.

Madde 11- Madde ile ilgili mevzuat kapsamında bir kamu kurum veya kuruluşuna karşı zorunlu hizmet yükümlülüğü bulunanların Başkanlıkta geçen hizmet sürelerinin, ilgili kurumun muvafakati ile söz konusu hizmet yükümlülüğünden sayılabilmesi öngörülmektedir.

Madde 12- Madde ile Başkanlıkta görev alanlar ile Başkanlıktan herhangi bir nedenle ilişiği kesilenlerin yükümlülüklerine yer verilmektedir.

Madde 13- Madde ile Başkanlık tarafından yürütülen görev ve faaliyetler kapsamında edinilen sırların saklanmasına ilişkin yükümlülükler düzenlenmektedir.

Madde 14- Madde ile Başkanlığın gelir kalemleri belirlenmektedir.

Madde 15- Madde ile Başkanlığın hizmetlerini yürütürken ihtiyaç duyacağı her türlü araç, malzeme gibi hususlar yönüyle tabi olduğu muafiyet ve istisnalar belirlenmektedir.

Madde 16- 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda bazı suçların bilişim sistemleriyle işlenmesi, suçun nitelikli hali (madde 142, madde 158, madde 228) olarak düzenlenmektedir. Aynı Kanunun 243 ila 246 ncı maddelerinde ise "Bilişim Alanında Suçlar" başlığı altında özel bir bölüm yer almaktadır. Türk Hukuk Sisteminde siber suçlarla ilgili olarak farklı kanunlarda da çeşitli düzenlemeler olduğu görülmektedir. 5/12/1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanununda siber suçlara konu olabilecek eylemler düzenlenmektedir. Yine siber suçların internet ortamında artan oranda işlenmesi, internetle alakalı bazı özel kurumların oluşması ve belli bir düzenin geliştirilmesi 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile belirlenmekte, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla, yer ve erişim sağlayıcılar üzerinden mücadeleye ilişkin esas ve usuller düzenlenmektedir.

Öte yandan;teknolojik gelişmelerle birlikte kritik altyapılara yönelik tehditlerin artması ve siber olayların daha karmaşık hale gelmesi nedeniyle, bu alanın tekrar gözden geçirilmesi ve farklı bir bakış açısıyla ele alınması elzemdir.

Bu nedenle madde ile, siber güvenliğe ilişkin caydırıcı yaptırım süreçlerinin işletilmesine yönelik olarak; bazı fiillere (siber saldırı gerçekleştirilmesi, kişisel veya kurumsal verilerin sızdırılması, sızdırılan verilerin yayılması vb.) hapis cezası, diğer bazı fiillere ise (mevzuatın öngördüğü tedbirlerin alınmaması, denetim faaliyetlerinin engellenmesi vb.) idari para cezası verilmesi düzenlenmektedir.

Madde 17- Madde ile Başkanlık tarafından verilen idari para cezalarının uygulanmasına ilişkin esaslar belirlenmektedir.

Madde 18- Madde ile Kanun kapsamında kamu kurum ve kuruluşlarının sağladığı destekle kurulan, geliştirilen veya desteklenen siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerin yurt dışına satışı ile bunları üreten şirketlerin bölünme, birleşme, pay devri veya satış işlemleri Başkanlığın uygun görüşüne tabi kılınmaktadır.

Milli güvenlik ve kamu kaynaklarının verimli kullanımı amacıyla, kamu kurum ve kuruluşları ve kritik altyapıların bilişim sistemlerinde, yeni tedarik sözleşmeleri kapsamında kullanılacak siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerin yurt dışına satışı veya bunları üreten şirketlerin bölünme, birleşme, pay devri veya satış işlemlerinin onayına ilişkin usûl ve esasların Başkanlık tarafından belirleneceği hüküm altına alınmaktadır.

Madde 19- Madde ile diğer ilgili bazı Kanun ve Kanun Hükmünde Kararnamelerde uyum düzenlemelerinin yapılması öngörülmekte, bu kapsamda 5018, 5809 ve 5651 sayılı Kanunlar ile 375 sayılı Kanun Hükmünde Kararnamede muhtelif düzenlemeler yapılmaktadır.

Geçici Madde 1- Madde ile Kanunun yürürlüğe girmesiyle ilgili uyum, geçiş ve kuruluş işlemlerine ilişkin düzenlemelerin belirlenmesi sağlanmaktadır.

Madde 20- Yürürlük maddesidir.

Madde 21- Yürütme maddesidir.

Milli Savunma Komisyonu Raporu

Türkiye Büyük Millet Meclisi
Milli Savunma Komisyonu *22/01/2025*
Esas No: 2/2860
Karar No: 6

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

2/2860 esas numaralı, "Siber Güvenlik Kanunu Teklifi", Komisyonumuzun 15/1/2025 tarihinde yaptığı 5'inci toplantısında görüşülmüş ve kabul edilmiştir.

Raporumuz, Genel Kurulun onayına sunulmak üzere Yüksek Başkanlığınıza saygı ile arz olunur.

1. Giriş

Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin; Siber Güvenlik Kanunu Teklifi 10/1/2025 tarihinde Türkiye Büyük Millet Meclisi Başkanlığına sunulan ve Başkanlıkça aynı tarihte tali komisyon olarak Adalet Komisyonu, Plan ve Bütçe Komisyonu ile Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonuna, esas komisyon olarak da Komisyonumuza havale edilen 2/2860 esas numaralı "Siber Güvenlik Kanunu Teklifi", Komisyonumuzun 15/1/2025 tarihli 5'inci toplantısında; Kanun Teklifinin ilk imza sahibi Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile Milli Savunma Bakanlığı, Hazine ve Maliye Bakanlığı, Adalet Bakanlığı, İçişleri Bakanlığı, Sanayi ve Teknoloji Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, Ticaret Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Rekabet Kurumu, Cumhurbaşkanlığı Genel Sekreterliği Personel ve Prensipler Genel Müdürlüğü, Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile Türkiye Odalar ve Borsalar Birliği Türkiye Yazılım Meclisi ve Türkiye Bilişim Derneği yetkililerinin de katılımlarıyla görüşülmüştür.

Komisyonumuzun söz konusu Teklif ile ilgili müzakereleri tutanağa bağlanmış ve toplamda 37 sayfa tam tutanak tutulmuştur.[1]

2. Teklifin İçeriği

Bu Kanun Teklifi ile; 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 dair esasların düzenlenmesi amaçlanmaktadır.

3. Teklifte Öngörülen Düzenlemeler

2/2860 Esas Numaralı Kanun Teklifi ile;

- Ülkemizin siber güvenlikle ilgili politika ve stratejisini belirlemek üzere Siber Güvenlik Kurulunun kurulması,

- Siber güvenlik alanında geliştirilen politikaların ulusal satıhta etkin bir şekilde uygulanması,

- Kamu kurumları ile kritik altyapı kuruluşlarının siber mukavemetinin ve siber olgunluk seviyesinin artırılması,

- Güncel teknolojik gelişmelerin takip edilmesi ve siber güvenlik süreçlerine entegre edilmesi,

- Kamu kurumları ve kritik altyapı kuruluşlarının bilişim sistemlerinde oluşabilecek siber güvenlik olaylarının merkezi bir bakış açısıyla izlenmesi, tespiti ve bertaraf edilmesi,

- Eylem planlarının ve ikincil mevzuatların hayata geçirilmesi,

- Denetim ve özellikle caydırıcı yaptırım süreçlerinin işletilmesi,

- Siber güvenlik ekosisteminin güçlendirilmesi,

- Standardizasyon, sertifikasyon ve yetkilendirme süreçlerinin düzenlenmesi,

- Siber suçlara yönelik cezaların artırılması suretiyle caydırıcılığın sağlanması,

amaçlanmaktadır.

---

[1] *Komisyonun toplantı tutanaklarına aşağıdaki bağlantı adresinden ulaşılabilir: https://www.tbmm.gov.tr/Tutanaklar/TutanakGoster/4079*

4. Komisyonda Teklif Üzerinde Yapılan Görüşmeler

a) Anayasaya aykırılık iddiası:

Komisyon üyesi Çanakkale Milletvekili Özgür CEYLAN; görüşmelere başlamadan Anayasa'ya aykırılıkla ilgili bir görüşme talepleri olduğunu belirtmiş, kendisinin yerine Anayasa Komisyonu üyesi Aydın Milletvekili Süleyman BÜLBÜL'e söz verilmesini istemiştir.

Aydın Milletvekili Süleyman BÜLBÜL; Hukuk devleti açısından hukuki belirlilik ve ölçülülük ilkesinin önemli bir husus olduğunu, Kanun teklifinin 8'inci maddesinin beşinci fıkrasının Anayasa'ya uygunluk konusunda sorunlu olduğu düşündüklerini, burada Anayasa'nın açık bir maddesi olan 9'uncu ve 13'üncü maddelerine aykırı olarak yargı yetkisinin ihlal edildiğini,

Bir memur ve atanan bir kişi olan Başkana, hâkim kararı dışında verdiği yazılı emirle, konutta, iş yerinde ve kamuya açık olmayan kapalı alanlarda arama yetkisi, kopya çıkarma yetkisi, el koyma yetkisi vermenin açıkça hâkim kararı olmadan yargı yetkisine müdahale anlamına geldiğini,

Kanun yapma tekniğinde kanun teklifinin muğlak olmaması gerektiğini, "gecikmesinde sakınca bulunan hâller" ibaresinin Anayasa'nın 2'nci, 7'nci, 8'inci, 9'uncu ve 13'üncü maddelerine aykırı olduğunu,

Arama kararının içeriğinin neye göre belirleneceğinin Ceza Muhakemesi Kanunu'nun 119'uncu maddesinin (2)'nci fıkrasında açıkça belirtildiğini, "Arama karar veya emrinde; aramanın nedenini oluşturan fiil, aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya, karar veya emrin geçerli olacağı zaman süresi açıkça gösterilir." denildiğini,

16'ncı maddenin (5)'inci fıkrasındaki "Siber uzayda veri sızıntısı olmadığı halde veri sızıntısı yapılmış gibi bu yönde algı oluşturmak suretiyle kurumları veya şahısları hedef almaya yönelik faaliyet yürütenlere iki yıldan beş yıla kadar hapis cezası verilir." hükmündeki "veri sızıntısı olmadığı halde" ve "hedef almaya yönelik faaliyet yürütenler" ifadelerinin, uygulamada ne şekilde tespit edileceğinin açıklanmamış olmasının, hukuki belirlilik ve ölçülülük ilkelerine ve Anayasaya aykırı olduğunu,

dile getirmiştir.

Hakkâri Milletvekili Onur DÜŞÜNMEZ; Anayasa Mahkemesi'nin aynı konuda iptal kararı verdiği Kanun Teklifinin 7'nci maddesinin, Anayasa'nın 20'nci maddesine açıkça aykırılık teşkil etmekte olduğunu ve bu yönüyle kanun metninden çıkarılması gerektiğini düşündüklerini,

8'inci maddenin beşinci fıkrasında mevzuatın kolluğa tanımadığı bir yetkinin burada Kurul Başkanına verilmesinin Ceza Muhakemesi Kanunu'nun açıkça ihlali olduğunu,

Kanun teklifinin 12'nci maddesinin de Anayasa 48'deki çalışma hürriyetine aykırılık teşkil ettiğini düşündüklerini,

16'ncı maddenin beşinci fıkrasının, Türk Ceza Kanununun 217/A Maddesinde düzenlenen "bilgiyi alenen yayma suçunu" delen yeni bir madde ekleme tekniğinin hem Anayasa'ya hem de ceza hükümlerine aykırı olduğunu, bu itibarla 16'ncı maddenin beşinci fıkrasının, altıncı fıkrasının ve fıkradaki muğlak bilgiler sebebiyle de dokuzuncu fıkrasının kanun metninden çıkarılmasını teklif ettiklerini,

dile getirmiştir.

Teklif sahibi ve Afyonkarahisar Milletvekili Ali Özkaya Anayasa'mızın 20, 21 ve 22'nci maddelerinin kişi dokunulmazlığı, ifade özgürlüğü, arama, konut araması gibi hususlarda Anayasa'da belirtilen sebeplerle ve Anayasa'nın 13'üncü maddesi kapsamındaki demokratik toplumun gerekleri, kanunilik ve ölçülülük, orantılılık ilkeleri çerçevesinde yasal hakların sınırlanabileceğini yazdığını,

Aslında kanun teklifinin getirilişindeki ilk mantık ve amacın bir siber saldırı olduğunda bir suç soruşturmasından daha önce ve öncelikle bunu önlemek ve durdurmak olduğunu, polise tanındığı gibi, önleme araması ve arama yaparak o dijital materyallerin kanun kapsamında olanlarla ilgili kısımlarına el koyma mantığı olduğunu,

Bu fiillerin aynı zamanda bir suç da oluşturabileceğini ancak hangi aşamanın önleme, hangi aşamanın ceza soruşturmasına geçtiği tam olarak belli olmayacağı için ibarenin başına Anayasa'nın 20, 21, 22'nci maddesindeki sınırlama ve amaçlar çerçevesinde "Cumhuriyet Savcısı veya Başkanın..." ibaresinin eklenmesi şekliyle Komisyonun takdirine sunacaklarını,

cevaben Komisyona ifade etmiştir.

Görüşmelerin ardından yapılan oylamada Anayasa'ya aykırılık iddiası kabul edilmemiş ve görüşmelere devam edilmiştir.

b) Kanun Teklifinin ilk imza sahibi Afyonkarahisar Milletvekili Ali Özkaya tarafından yapılan açıklamalarda;

Dijitalleşmenin dünyada da ülkemizde de çok hızlı bir şekilde gelişip değiştiğini,

Ülkemizde bu konuyla ilgili birden çok kanunda hüküm bulunduğunu, internet ortamında işlenen suçlarla ilgili 2007'de çıkarılan ve çok kere değişiklik yapılan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun yanında 5809 sayılı Elektronik Haberleşme Kanununun bulunduğunu,

Ulaştırma ve Altyapı Bakanlığının ve Bilgi Teknolojileri ve İletişim Kurumunun ilgili birimleri yanında her bakanlığın kanunlarında kendi bilgi işlem kurumlarıyla ilgili hükümler bulunduğunu, dolayısıyla, mevzuatta bir dağınıklık yaşandığını,

Bunların bir bütün hâlinde ve tek bir çatı altında derlenip toparlanmasının ülkenin siber güvenliğinin daha sıkılaştırılması, ekosisteminin daha düzgün bir şekilde kurulması, siber ürünlerle ilgili sertifikasyon, standardizasyonun sağlanması ve bu konudaki denetimlerin yapılmasının önemli bir ihtiyaç olduğunu,

Kanun Teklifinin kural olarak kamu kuruluşlarının tamamını kapsadığını, Emniyet Genel Müdürlüğünün ve Jandarma Genel Komutanlığının yalnızca istihbarat faaliyetleri ile Milli İstihbarat Teşkilatı'nın kuruluş amacı tamamen istihbarat olduğu için MİT Kanununun bu kanun kapsamının dışında kabul edildiğini, Emniyetin ve Jandarmanın istihbarat dışındaki bütün faaliyetlerinin de bu kanunun kapsamı dâhilinde olduğunu,

177 sayılı Cumhurbaşkanlığı Kararnamesi ile Siber Güvenlik Başkanlığının kurulduğunu, Kanun Teklifi ile kurulması öngörülen Siber Güvenlik Kurulunda ise Cumhurbaşkanı veya Yardımcısı Başkanlığında Adalet Bakanı, İçişleri Bakanı, Dışişleri Bakanı, Millî Savunma Bakanı, Ulaştırma Bakanı, Siber Güvenlik Kurulu Başkanı, Savunma Sanayii Başkanı ve MİT Başkanı gibi üst makamların yer alacağını,

Bu Kurul'un, Başkanlık ile kamu kurumları arasında "Burası benim gizlilik alanımdır, buraya girmeyin." denildiğinde ortaya çıkan ihtilafları gidereceğini, Kurulun verdiği kararlar çerçevesinde siber güvenlik faaliyetlerinin yürütüleceğini,

Başkanlık kurulduktan sonra Bilgi Teknolojileri ve İletişim Kurumunun içindeki bir kısım görevlerin bu kuruma devredileceğini, Kurum, Kurulun Başkanı, kurulun uzmanları, kamu kuruluşlarında ve siber güvenlikle ilgili kanun kapsamına giren özel kuruluşlarda da denetim faaliyetlerini kendileri veya yetkilendirilmiş uzman veya şirketler eliyle yürüteceğini,

Kamu kuruluşlarında bir denetim olacaksa mutlak surette Kurulun uzmanları ve onların yanında gerekiyorsa yetkili özel kişilerin olacağını, yani özel sertifikalı kişilerin bir kamu kuruluşuna asla gidip de denetleme yapmayacağını, Devletin esas fonksiyonlarından biri olan denetim yetkisinin yine devlet eliyle yürütülmüş olacağını,

Siber güvenlik konusunda ülkelerde ciddi ve sıkça saldırılar yaşandığını, finans kuruluşlarından enerji altyapılarına, bankacılıktan diğer kuruluşlara kadar sürekli saldırıların olduğunun veyahut da saldırı olduğu iddiasının, algısının oluşturulduğunun çok yaygın bir şekilde gündeme geldiğini,

Geçen yıl TCK 217/A'da düzenlenen " halkı belirli bir şekilde yönlendirmeye matuf ve sosyal medyadaki algı ve dezenformasyon oluşturma" suçunun kapsamının ve suçun unsurlarının çok ağır olduğunu ancak kapsamının da çok dar kaldığını, bugünkü sosyal medya ve dünyada dijitalin geldiği noktada mevcut suç tanımının bu konuyu karşılamadığını, dolayısıyla, burada bir değişikliğe ve yeni bir ilave hükme ihtiyaç olduğunu, Komisyon ve Meclis Genel Kurulunun suçun unsurlarını, ceza miktarlarını takdir ve tayin etmeye yetkili olduğunu,

Ülkemizde bugün itibarıyla 93 milyon mobil abonenin 72,7 milyonun geniş bant abonesi, 19,9 milyon da sabit geniş bant abonesi bulunduğunu, konvansiyonel savaşların yerini hibrit ve asimetrik savaşlara bıraktığını, devlet destekli siber saldırılar başta olmak üzere terör örgütleri, organize suç örgütleri, bireysel motivasyon ile hareket eden siber tehdit aktörleri tarafından devlet kurumları, enerji, fınans, sağlık, haberleşme sistemleri ve kritik altyapıların her türlü teknolojik cihazlarla hedef alınmaya başlandığını,

Cumhurbaşkanlığı Dijital Ofisi tarafından yapılan çalışmalarda dünyanın birçok ülkesinde dünya ülkelerinin çok büyük kısmında merkezî bir otoritenin kurulduğunu, merkezî otoritenin standardizasyonu, sertifikasyonu ve denetlemeyi yaptığını, bunların bizim ülkemize de getirilmesiyle birlikte bu alandaki kamusal açıklarımızın ciddi manada önleneceğini düşündüğünü,

Yine eğer bir siber güvenlik ürünü üreten yazılım, donanım yapan şirketler, özel şahıslar varsa ve bu kamu destekleriyle bir ürün geliştirilmişse bu ürünün yurt dışına ihracatıyla ilgili belirli sınırlamalar ve kurumdan izin almayı getirdiklerini, Devlet olarak birçok ülkeden bu ürünleri alırken ciddi manada sıkıntılarla karşı karşıya geldiğimizi,

Bu nedenle devletimizin geliştirdiği bu ürünlerin belirli bir izin dâhilinde satılmasını öngördüklerini, "Özel ticarete, özel teşebbüse engel olur mu?" şeklinde endişe ve tereddütlerin de giderileceğini, yani mevcut devam eden sözleşmelerden değil bundan sonraki yenilerle ilgili uygulanması gerektiğini öngördüklerini,

Kanun çıktıktan sonra siber güvenlik ürünü üreten şirketler, vakıf, dernek işletmeleri dâhil herkesin bu kanuna uyması gerektiğini, uymayanlar için hem hapis cezası hem de Başkanlık tarafından bunların ticaret sicilinden ilgili birimlerinin silinmesi, vakıf ve derneklerin de kapatılması yönünde mahkemeye müracaat edilmesiyle ilgili düzenlemeler olduğunu,

ifade etmiştir.

c) Kanun Teklifinin tümü üzerinde müzakerelerde milletvekilleri tarafından yapılan açıklamalarda;

Çanakkale Milletvekili Özgür CEYLAN; Siber güvenlik alanında geç de olsa bu düzenlemenin yapılmasının olumlu olduğunu partileri adına ifade ettiğini ancak maddelerde çekinceleri olduğunu, bunları ilerleyen maddelerde de tek tek konuşacaklarını, bu konunun Millî Savunma Komisyonu olarak Komisyonumuzda değerlendirilmesinden de duyduğu memnuniyeti ifade etmek istediğini,

Konunun tali komisyonlarda görüşülmediğini, bu yönüyle eksik kaldığını hatta Güvenlik ve İstihbarat Komisyonu'ndan da görüş alınması gerektiğini, bu Komisyonun üyesi İstanbul Milletvekili Yüksel Mansur KILINÇ'ın da bugün Komisyonda konuşacağını,

Siber Güvenlik Kurumunun denetlemesi konusunda "Bir Meclis ayağı var mı?" sorusunu sormak istediğini, Millî İstihbarat Teşkilatı ve diğer istihbarat kurumlarının da Meclise hesap verdiklerini, bu Komisyona Siber Güvenlik Kurumunun da hesap vermesi gerektiğini,

Hazır Milli Savunma Bakanlığı temsilcileri de buradayken özellikle Millî Savunma alanında Türk Silahlı Kuvvetlerinin ve içinde bulunduğumuz millî savunma sisteminin çok önemli sorunları olduğunu belirterek bunları da kısaca ifade etmiştir.

Hatay Milletvekili Adnan Şefik ÇİRKİN; böyle bir kurumun kuruluşunun ülkemizin gerek terörle mücadele ve gerek kurumlarımızın korunması adına son derece olumlu olduğunu, İYİ Parti olarak bu yasayı desteklediklerini, itiraz ettikleri noktalar da bulunduğunu ama genel anlamda bu yasanın ülkeye, devlete, millete faydalı bir yasa olacağına inandıklarını,

Suriye'de bir yönetim değişikliğini müteakip gelişen çeşitli olayların, yaklaşık on dört senedir kendi seçim bölgesi olan Hatay'ı birinci dereceden ilgilendirdiğini ve etkilediğini, on dört yıllık savaş hâlinin Hatay'a tahribatının çok büyük olduğunu,

Son deprem felaketinde toplam hasarın, toplam can kaybının, toplam ölü ve toplam yaralıların yüzde 50'sini bünyesinde taşıdığını, Hatay'ın böyle bir oranla karşılaşarak çok ağır bir darbe aldığını,

Suriye'de yönetimde el değişikliği yaşandığını, bu el değişikliğini müteakiben mevcut HTŞ kadrolarına atfedilmeyecek bazı olayların gelişmekte olduğunu, bunun da Hatay, Adana ve Mersin'de bazı huzursuzluklara sebep olduğunu, yaklaşık on dört yıllık savaşın sonunda şu anda Suriye'yi cihatçı ve selefi dinî görüşe sahip bir idarenin yönettiğini,

Suriye'de Alevilerin de yaşadığını ve Suriye Alevilerinin uzantısı olarak Türkiye'de Hatay, Adana ve Mersin'de 1 milyona yakın Alevi vatandaşlarımızın bulunduğunu, bunların akraba olduğunu ve şu anda Lazkiye'de pek o kadar olmasa da Hama ve Humus'ta oluşan bir çeteleşme sonucunda Alevi vatandaşların canına, malına ve namusuna tasallutun söz konusu olduğunu,

Bunun da Türkiye'yi ilgilendiren bir durum olduğunu, bunun farklı mahzurlarının da ileride karşımıza çıkacağını, Suriye'de yönetimi devralan zihniyetin Türkiye'ye eskiden olduğu gibi, yönetimi devralmadan evvel olduğu gibi ihtiyacının kalmadığını,

Suriye'de Batılı ülkelerin ve Arap devletlerinin hükmünün daha fazla geçmesi ihtimalinin söz konusu olduğunu, Suriye savaşının en büyük sıkıntısını çekmiş ülke olan Türkiye'nin bunlara hazırlıklı olması gerektiğini,

Suriye'de bundan sonra gelişecek her olumsuzluğun Türkiye'nin de sırtına bir yük olarak bineceğini, Türkiye'nin bu konuda dikkatli olması ve olayları çok yakından takip etmesi gerektiğini,

ifade etmiştir.

Zonguldak Milletvekili Eylem Ertuğ ERTUĞRUL; Yunanistan'ın 12 ada ve diğer adaların egemenliğini kendine bağlaması, uluslararası anlaşmalarla devredilmemiş olan adalarda, kayalıklarda ve adacıklarda bazı çalışmalar yapması, buralarda belediyeler kurup seçimler yapması, Yunanistan İçişleri Bakanlığı internet sitesinde bu seçim sonuçlarının yayınlanması gibi konularda Millî Savunma Komisyonu üyelerine vatandaşlardan çok fazla soru geldiğini,

Bu konuda, 7 Kasım 2024 tarihinde kendisinin Yunanistan'ın artan faaliyetleri karşısında Türkiye'nin atabileceği adımların değerlendirilmesi, yetkili makamların bu konudaki tepkisizliğinin sebeplerinin araştırılması ve neden bu ihlallerinin gerçekleştiği, bunlara yönelik neler yapılabileceğine dair bir genel görüşme açılması önerisi olduğunu, bu önerinin Cumhur İttifakı'nın oylarıyla, AKP ve MHP'nin ret oylarıyla reddedildiğini,

Dün, Milliyetçi Hareket Partisi Genel Başkanı Sayın Devlet BAHÇELİ'nin grup konuşmasında "12 ada gasp edilmiş, asıl sahibi olan Türk milletinden ayak oyunlarıyla çalınmıştır. Türkiye 12 adasız yaşasa bile 12 adanın Türkiyesiz yaşaması tam bir hayaldir." cümlelerini kullandığını hatta "Adaların silahlandırılmasının Türkiye'ye meydan okumaktır." şeklinde açıklamalar yaptığını,

Bu noktada, bu çalışmalarda biraz daha samimiyet olması gerektiğini düşündüğünü, muhalefetin verdiği her önergenin yanlış olmadığını, aynı şeyin Genel Başkan Yardımcısı, emekli Tümamiral Yankı BAĞCIOĞLU hakkında soruşturma açılması olayında da karşılarına çıktığını,

2021 yılı içerisinde Montrö'yle ilgili bir sıkıntı yaşadıklarını, o zamanki Meclis Başkanının "Nasıl Sayın Cumhurbaşkanı 'Ben İstanbul Sözleşmesi'nden çıkıyorum.' kararını verdi ve çıktı, aynı şekilde Montrö'den de çekilebilir." şeklinde bir açıklamada bulunduğunu, emekli amiraller ve bazı Dışişleri diplomatları bir deklarasyon yayınladıklarını, bunun çok büyük bir hata olacağını ifade ettiklerini, bu insanlara da çok büyük tepkiler gösterildiğini, yargılanmaya çalışıldığını, fakat sonraki süreçte Montrö Antlaşması'nın sayesinde özellikle Rusya-Ukrayna çatışmaları esnasında ne kadar yararlı olduğunu,

Aynı şekilde, teğmenler mevzusunda da, herhangi bir resmî görevi olmayan insanların kendi aralarındaki bir grup içerisinde yaptıkları bir konuşmanın delil olarak kullanılarak soruşturma açılmaya çalışıldığını, bu gibi noktalarda da samimiyet eksikliği olduğunu düşündüğünü,

dile getirmiştir.

Yüksel Mansur KILINÇ (İstanbul) Türkiye Büyük Millet Meclisinde Güvenlik ve İstihbarat Komisyonunda Cumhuriyet Halk Partisinin sözcüsü olarak görev yaptığını, görüşülen yasa teklifinin güvenlikle ilgili olduğunu, üyesi bulunduğu Komisyonu doğrudan ilgilendirdiğini, Güvenlik ve İstihbarat Komisyonunun tali komisyon olarak değerlendirilmemiş olması nedeniyle genel değerlendirmesini burada yapacağını,

Türkiye'de yakıcı bir siber güvenlik sorunu olduğunu, bunun Türkiye kamuoyunda sürekli anlatıldığını, bu konunun Genel Kurul görüşmelerinde ivedilikle ele alınması ve yerli güvenlik altyapısı da kurularak dünyanın yeni yaklaşımların ve yeni güvenlik önlemlerinin üzerinde çalışılması gerektiğini,

En son 2023'te Türkiye'nin Millî Güvenlik Siyaset Belgesinin güncellenmesine de eklendiğini, Mecliste Dijital Mecralar Komisyonunda da konuşulduğunu, burada büyük bir gecikme ve ihmallerimiz olduğunu,

Dezenformasyonla Mücadele Yasası Teklifinin Türkiye Büyük Millet Meclisine getirildiğini, Komisyonda Genel Kurula sunulduğunu ama görüşülmesinin bir süre ertelendiğini,

Bu arada bir İletişim Başkanlığı tarafından Dezenformasyonla Mücadele Merkezi kurulduğunu, bugünün tarihinin 15 Ocak olduğunu, yasa oluşumu beklenmeden 8 Ocak günü bir kararnameyle Siber Güvenlik Başkanlığının kurulduğunu,

Yasanın gerekliliği açısından sorular sorduklarını, bu sorulardan bir tanesinin kendisi tarafından Türkiye Büyük Milet Meclisine sorulduğunu ve Millî Savunma Bakanının yanıt verdiğini,

Sorunun, “Check Point Software Technologies adlı İsrail menşeli siber güvenlik şirketinin güvenlik duvarı yazılımını kullandığına dair haberler medyada yer almıştır; bu doğru mu?” şeklinde olduğunu, Milli Savunma Bakanlığının “Kullanımı sonlandırılmış olan bahse konu ürün haricinde Genelkurmay Başkanlığı ve bağlılarında bulunan kritik sistemlerde İsrail menşeli siber güvenlik ürünü kullanılmamaktadır.” denildiğini,

Hâlâ basın kartı sahibi olan bir milletvekili olarak benzer bir durumun bu yasa teklifi kanunlaştıktan sonra 16’ncı maddenin beşinci fıkrasında ne anlama geleceğini sormak istediğini, yasanın gerekli olduğunu ama bu yasa teklifinin hazırlanması sırasında aynı zamanda kurulan kurumun denetiminin de nasıl yapılacağının gösterilmesi gerektiğini,

2014 yılında Türkiye Büyük Millet Meclisinde Güvenlik ve İstihbarat Komisyonunun MİT Kanunu’nda yapılan bir değişiklikle kurulduğunu, ana gerekçelerden bir tanesinin “Güvenlik alanı kontrol edilemez bir alan dolayısıyla bu alanın Türkiye Büyük Millet Meclisi tarafından denetlenmesi lazım. Kişisel verilere erişen bu güvenlik kurumlarında kişisel verilerin ihlalinin önlenmesi için denetim gerekir.” şeklinde olduğunu, bundan dolayı Türkiye Büyük Millet Meclisinde Güvenlik ve İstihbarat Komisyonu kurulduğunu ve devletin güvenlik ve istihbarat faaliyetini yürüten kurumların yine güvenlik ve istihbarat faaliyetlerinin denetlenmesini sağlayıcı bir düzenleme yapıldığını,

Kanunun içinde Millî İstihbarat Başkanlığı, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Maliye Bakanlığıyla bağlantılı kurum olan MASAK’ın bulunduğunu, bu Komisyon tarafından Cumhurbaşkanlığı eliyle denetlenmesinin sağlandığını,

Bir güvenlik kurumu olarak Siber Güvenlik Başkanlığının kurulduğunu, Siber Güvenlik Başkanlığının da güvenlikle ilgili veriler ve faaliyetler, istihbarata dair değerlendirmeler ve bilgiler, kişisel verilerin korunması gibi konularda Türkiye Büyük Millet Meclisi Güvenlik ve İstihbarat Komisyonunda denetlenebilir bir başkanlık olması gerektiğini, yasa teklifinde bunun yer alması gerektiğini,

Gerek işin bu yanı gerek yasa maddelerinin bir kısmında özellikle ilgili olduğunu gördüğümüz 16’ncı maddenin beşinci fıkrasında verilerin sızıntısıyla ilgili yaklaşıma da bakıldığında bu işin tesadüf olmadığını, esasen Siber Güvenlik Başkanlığının denetimden kaçınılmaya çalışıldığı sonucuna varabildiğini,

ifade etmiştir.

Eskişehir Milletvekili Utku ÇAKIRÖZER; Meclise ifade ve basın özgürlüğünü iyileştirecek hiçbir kanunun gelmediğini, Adalet ve Kalkınma Partisinin getirdiği her kanunda, her torbada demokraside, özgürlükler alanında adım adım kısıtlamaya, karartmaya gidildiğini, önümüzdeki Siber Güvenlik Kanunu Teklifinin de bunlardan sonuncusu olduğunu,

Gerekçesinde “Ülkemizin siber güvenlikle ilgili politika ve stratejisini belirleyeceğiz, siber güvenlik yaklaşımını yeniden yapılandıracağız.” denildiğini, bunlara ihtiyaç olduğunu ancak teklifin içeriğine bakıldığında başta ifade ve basın özgürlüğü olmak üzere, özel hayatın gizliliği, kişisel verilerin korunması gibi temel hak ve özgürlüklerin korunması açısından büyük risk ve tehditler barındırdığını,

Bu teklifin 2022 yılında dezenformasyonu önleyeceğiz denilerek Meclise getirilen ve Türk Ceza Kanununa halkı yanıltıcı bilgiyi alenen yayma suçunun eklendiği sansür yasasına benzediğini, siber tehdit, siber olay, veri sızıntısı, algı operasyonu gibi muğlak ve yasal olarak belirsiz ifadelerle tamamen keyfî uygulama ve yaptırımlara açık bir düzenlemeyle karşı karşıya olduklarını düşündürdüğünü, örneğin, “algı operasyonu” gibi belirsiz bir kavramın eleştirel haber yapan gazetecilerin veya sosyal

medyada fikirlerini paylaşan kişilerin kolaylıkla hedef alınmasına yol açabileceğini, bu tarz muğlak ifadelerin en başta demokratik toplumların temel değerlerinden biri olan öngörülebilirlik ve hukuki güvence ilkelerine aykırı olduğunu, maddelere bakıldığında ise teklifin 6'ncı, 8'inci ve 16'ncı maddelerinin ifade özgürlüğü, basın özgürlüğü, özel hayatın gizliliği ve kişisel verilerin korunması açısından ciddi sorunlar yaratabileceği hususunda genel bir algı bulunduğu, özellikle, veri sızıntısı olmadığı hâlde veri sızıntısı yapılmış gibi algı oluşturma suçu ve bu suçu işleyenlere iki ile beş yıl arasında hapis cezası öngörülmesinin basın özgürlüğüne yönelik sistematik bir tehdit olarak karşımıza çıktığını,

Teklifin 6'ncı maddesiyle Siber Güvenlik Başkanlığına kamu kurumları ve kritik altyapı kuruluşlarından veri ve Log kayıtlarını toplama, iki yıl süreyle saklama ve çalışma süresi sonunda imha yetkisi öngörüldüğünü, bu verilerin nasıl korunacağı, hangi koşullarda imha edileceği, kişisel verilerin kötüye kullanımının önüne nasıl geçileceği gibi konularda büyük bir belirsizlik olduğunu,

Gazeteciler için haber kaynaklarından alınan verilerin, belgelerin, kayıtların nasıl korunacağının bilinmediğini, bu düzenleme sadece gazetecilik için değil, özel hayatın gizliliği ve demokratik denetim için de oldukça kaygı verici olduğunu,

Siber Güvenlik Başkanlığına geniş yetkiler verilirken bu bilgilerin üçüncü kişilerce kötüye kullanım riskine karşı nasıl bir denetim olacağının bilinmediğini, teklifin 8'inci maddesinin (5)'inci fıkrasıyla Siber Güvenlik Başkanlığına gecikmesinde sakınca bulunan hâllerde hâkim onayı olmaksızın arama yapma, dijital materyallere el koyma ve veri toplama yetkisinin tanındığını,

Bu düzenlemenin de özellikle araştırmacı gazetecilik için büyük tehdit oluşturduğunu, Gazetecilerin haber kaynağından aldığı belgelerin, iletişim kayıtlarının bu yetki kapsamında erişilebilir hâle geleceğini, gazetecilerin haber kaynaklarının kendilerini baskı altında hissedeceğini,

Teklifin 16'ncı maddesinin (5)'inci fıkrasındaki metindeki "Siber uzayda veri sızıntısı olmadığı hâlde veri sızıntısı yapılmış gibi bu yönde algı oluşturmak suretiyle kurumları veya şahısları hedef almaya yönelik faaliyet yürütenlere iki yıldan beş yıla kadar hapis cezası verilir." Şeklindeki düzenlemeye göre, algı yaratılması gibi tamamen muğlak ifadelerin, eleştirel içerikler cezai yaptırıma neden olacağını, yine bu madde ile bu tür olayları sosyal medyadan tartışan yurttaşların cezalandırılmasının da mümkün olabileceğini,

Sansür yasası çıktıktan sonra iki yılda 4.590 kişi hakkında soruşturma açıldığını, bunlardan 384'ünün davaya çevrildiğini, bu soruşturma açılanlardan en az 56 gazeteci hakkında 66 farklı soruşturma açıldığını, 7 gazetecinin tutuklandığını, şimdi bu soruşturmalara, bu davalara, bu tutuklamalara yenilerini ekleyecek bir hukuki altyapının oluşturduğunu,

Yapılacak şeyin muhalefetle, basın meslek örgütleriyle, sivil toplumla bir araya gelinip, onların görüşleri alınarak bu teklifin yeniden değerlendirilmesi ve riskleri ortadan kaldıracak, bertaraf edecek bir düzenlemenin geçirilmesi olduğunu,

dile getirmiştir.

Türkiye Odalar ve Borsalar Birliği, Türkiye Yazılım Meclisi Başkanı Ertan BARUT;

Türkiye özel sektörünün en büyük çatı kuruluşu Türkiye Odalar Borsalar bünyesinde yazılım sektörü adına faaliyet yürüten Türkiye Yazılım Meclis Başkanı olarak Meclislerini temsilen geldiğini, Komisyona davet edildikleri ve görüşlerini aktarma fırsatı sağladığı için de teşekkür ettiklerini,

Siber Güvenlik Başkanlığı kurulmasını ve hazırlanmış olan bu kanun teklifini millî güvenlik, kamu düzeni ve kritik altyapıların siber tehditlere karşı korunması açısından kritik ve tarihî bir adım olarak nitelendirdiklerini ve desteklediklerini,

Diğer taraftan, siber güvenlik sektörünün her ne kadar savunma sanayisiyle ilişkilendirilse de çok daha geniş bir ekosisteme ve müşteri tabanına sahip olan bilişim sektörünün altında yer alan sivil bir ticari sektör olduğunu, bütün dünyada da bu şekilde yani bilişim sektörünün altında yer aldığını,

Ülkemizde binler mertebesinde olan yerli siber güvenlik firmaları bulunduğunu, 50 bini aşkın çalışan ve 100 binlerin üzerinde de kurumsal müşterileri olduğunu, bu firmaların ve aynı zamanda tabii ki internet kullanıcıları açısından bakıldığında da milyonları aşan bireysel müşteri tabanı bulunduğunu,

Bunların yanında ülkemizin ihracatına, uluslararası bilinirliğine ve rekabet gücüne büyük katkısı olan bilişim, iletişim ve yazılım sektörünün uluslararası rekabet gücünü korumak, yabancı ve yerli yatırım imkânlarını artırmak ve yenilikçi girişimlerin büyümesini teşvik etmenin de son derece önemli olduğunu,

ifade etmiştir.

ç) Komisyonda milletvekilleri tarafından sorulan ve yapılan açıklamalara cevaben;

Afyonkarahisar Milletvekili Ali ÖZKAYA; 8'inci maddedeki denetimle ilgili kısımda makul ve Anayasa'ya uygun bir değişikliği Komisyonun değerlendireceğini, gazetecilikle veyahut da basınla ilgili kısmın da eğer çok geniş olduğu düşünülüyorsa Komisyonun takdirini ortaya koyacağını ve daha belirli, suçun unsurlarının belirli olduğu bir hâle getirileceğini,

Mevcut Kanunun 217/A maddesinde bir boşluk bulunduğunu sosyal medyadaki ve dijital mecralardaki bu suçları karşılamadığını,

Denetim konusunda, tüm kamu kuruluşlarının her birinin tek tek Meclisin denetimi altında olmasının sistemimiz açısından sınırlı olduğunu, Meclisin genel yürütmenin denetimini yaptığını, bu kurulun da denetiminin Cumhurbaşkanlığı, Devlet Denetleme Kurulu ve diğer kurumlarca yapılacağını,

Siber Güvenlik Kurulunda 7 Bakanın yer aldığını ve bu kadar çok bakanın olduğu bir yerde denetimin daha sıkı olacağı kanaatinde olduğunu,

ifade etmiştir.

d) Kanun Teklifinin maddeleri üzerinde müzakerelerde milletvekilleri tarafından yapılan görüşmelerde;

3'üncü madde üzerinde yapılan görüşmelerde,

Kritik altyapı işleten kuruluşlar için teklifle birçok yükümlülük getirilmiş olmakla beraber bu kritik altyapıların neler olduğunun belirlilik ve öngörülebilirlik ilkeleri ve gereği kanunda ifade edilmesi gerektiği şeklindeki görüşe cevaben,

Kritik altyapı kavramının hızlı değiştiği, dinamik hayatta statik kanunları değiştirmenin zorluğu nedeniyle bu belirlemenin Kurulun yetkisinde olmasının daha doğru olduğu ve sektörel sorunlar yaşamanın önüne geçileceği ifade edilmiştir.

Siber Tehdit İstihbaratı tanımı içerisinde yer alan "zenginleştirilmiş bilgi" ifadesinin de muğlak olduğu dile getirilmiştir.

4'üncü madde üzerinde yapılan görüşmelerde,

"Siber güvenliğin sağlanmasına yönelik çalışmalarda öncelikle yerli ve millî ürünler tercih edilir." ibaresindeki öncelikle kelimesinin çıkarılarak tamamen yerli ürünlerin tercih edilmesi önerisine karşı cevaben,

Kamu kuruluşlarının ancak Siber Güvenlik Başkanının sertifika ve standardizasyon verdikleri ürünleri kullanabilecekleri, Türkiye'nin ihtiyacı olan olgunlaşmış bir siber güvenlik ürünü ülkemizde üretilmiyorsa bu ürünün kullanılacağı ifade edilmiştir.

5'inci madde üzerinde yapılan görüşmelerde,

Bu Kurumu kimin denetleyeceği konusundaki soru, Kurumun Cumhurbaşkanlığına bağlı olan Devlet Denetleme Kurulu tarafından denetleneceği ve özel bütçeli bir kuruluş olması dolayısıyla Sayıştay Başkanlığı denetimine de tabi olduğu şeklinde cevaplandırılmıştır.

6'ncı madde üzerinde yapılan görüşmelerde,

Siber Güvenlik Başkanlığına geniş yetkiler tanıyan bu teklifin, yalnızca bireylerin değil aynı zamanda kritik altyapıların verilerinin de yoğun şekilde toplanıp analiz edilmesine olanak tanıdığı, bu durumun özel hayata açık bir müdahale anlamına geldiği aynı zamanda bu bilgilerin üçüncü taraflarca kötüye kullanılma riskini de barındırdığı,

Siber ürünlere onay veren kurumun aynı zamanda tekrardan kullanılmasına onay vermesinin bürokrasiyi arttıracağı,

Cevaben ilk başta bir ürüne sertifika ve standardizasyon verileceği, daha üst versiyonlarda ve güvenlik alanlarında kullanmak için ilave bir ihtiyaç da olabileceği, düzenlemenin bu amaçla yapıldığı,

dile getirilmiştir.

7'nci madde üzerinde yapılan görüşmelerde,

Tüzel kişiliği bulunmayan kuruluşların ne olduğu noktasında bir açıklama yapılması talebi, bu tüzel kişilerin kendilerini "siber internet topluluğu", "siber internet birliği", "tescili olmayan siber internet vakfi", "topluluk" ve "platform" şeklinde tanımlayabilecek grupları kapsadığı şeklinde cevaplandırılmıştır.

8'inci madde üzerinde yapılan görüşmelerde,

Az önce değişiklikle ilgili önergenin geldiği ama bu değişikliğin de tam olarak ihtiyacı karşılamadığı, Anayasa Mahkemesinin bu konuda lehte ve aleyhte kararları bulunduğu, burada çok acil bir müdahale ihtiyacı olabileceği, hemen gitmek gerekebileceği ama bunun bizi asla hukuktan uzaklaştırmaması gerektiği,

8'inci maddenin, Siber Güvenlik Başkanlığına geniş yetkiler tanıdığı, bu yetkilerin nasıl kullanılacağı, hangi sınırlar içinde kalacağı ve bireylerin mahremiyetine nasıl saygı gösterileceğinin açıkça belirlenmesi gerektiği, Maddenin anayasal düzlemde ciddi soru işaretlerini barındırdığı,

Özellikle madde metninde Başkanlığın yetkileri, hâkim kararı olmaksızın konut ve iş yerlerinde arama, el koyma ve kopya çıkarma işlemlerinin gerçekleştirilebileceğinin düzenlendiği, bu hükmün, Anayasa'nın 21'inci maddesinde düzenlenen konut dokunulmazlığı ve 20'nci maddesinde güvence altına alınan özel hayatın gizliliği ilkeleriyle doğrudan çeliştiği,

Adli kolluğun kişileri gözaltına alabileceği, kişilerin suçtan elde edilen suç unsurlarına el koyma kararı verebileceği, Kurulun adli bir görevi olmayıp sadece idari bir Kurul olduğu, adli bir yetkinin idari bir kuruma verilmemesi gerektiği,

Bu maddenin Anayasa'ya aykırı olduğunu ve ilgili başvuruların da yapılacağı şeklindeki itirazlara karşı,

Anayasa'nın 20, 21 ve 22'nci maddeleri ile ilgili olarak, Anayasa'nın 13'üncü maddesine göre kişisel temel hakları sınırlamaya yönelik gerekçelerin ve Cumhuriyet Savcısının da metne eklendiği, örneğin gece saat üçte eğer elektrik, iletişim altyapımıza veya bir başka altyapımıza saldırı olduğunda buna o anda müdahale edilmezse daha büyük zararlarla karşılaşılacağı,

Bir suç örgütünün Türkiye'nin değişik yerlerinden, 30-40 yerden aynı anda bir siber saldırıya geçmesi durumunda 30-40 ayrı yerde gece saat üçte sulh ceza mahkemesinden arama kararı alınmasının, acilen müdahale edilmesinin ve bu siber saldırının durdurulmasının, bu teknolojiyle mücadele etmenin kolay bir iş olmadığı,

Teklifin sadece kendi amacıyla sınırlı bir bilgi almayı zorunlu kıldığı, sınırsız bir bilgi alma yetkisi tanımadığı, bir kamu görevlisinin bu yetkiyi aşarak suç işlerse mutlaka Ceza Kanunu'ndaki ve diğer kanunlardaki müeyyidelerle karşılaşacağı,

dile getirilmiştir.

9'uncu madde üzerinde yapılan görüşmelerde,

Teklifte öngörülen yönetmeliklerin bir takvim çerçevesinde bir an önce çıkarılarak koordinasyonun sağlanması gerektiği dile getirilmiştir.

10'uncu madde üzerinde yapılan görüşmelerde,

Kurumlar kadar kişilerin de her an siber tehditle karşı karşıya bulunduğu ortada iken tüm hayatımızı ilgilendiren bu dijital alanın denetlenebilir, güvenilir ve geliştirilebilir olması ve teklifin yaşanacak sorunların çözümünde yetki, görev, sorumluluk ve uygulama alanlarında kapsam dışı bir unsur kalmayacak şekilde, gerekli özenin gösterilerek detaylı bir çalışmayla hazırlanması gerektiği,

Siber güvenlik alanında istihdam edilecek personelin bu alanın her türlü risk ve tehlikesini bilen çok deneyimli insanlar olması gerektiği, uzman diyeceğimiz bu kişilerin özlük haklarının, çalışma koşullarının, hiyerarşik konumlarının ve işin mahremiyetiyle ilgili olarak teklifte daha net düzenlemeler olması gerektiği,

Teklifte "Bu kişilerin atanması, nitelikleri, görev ve sorumlulukları, disiplin hükümleri ve mali ve sosyal haklarının kanunda açık bir biçimde düzenlenmesi gerekir." denilirken ve bu esasların kanunla düzenlenmesi gerekirken Siber Güvenlik Kuruluna karar alma yetkisi tanınmasının Anayasa'nın 128'inci maddesine aykırı olduğu şeklindeki görüş ve itirazlara cevaben,

7315 sayılı Kanun'da kendi kuruluş kanunlarında güvenlik soruşturması isteyen Kurumların yazıldığı, bu nedenle çok kritik bir Kurum olacağı için hem arşiv araştırması hem güvenlik soruşturması yapılması gerektiği, bu Kuruma çok yetkin siber güvenlik uzmanlarının alınacağı ve maaşlarının da emsallerinden yüksek olacağı, bunların özel seçileceği ve sınırlı sayıda olacağı,

ifade edilmiştir.

12'nci madde üzerinde yapılan görüşmelerde,

Muvafakat verilmesinin yalnızca kamu kurumları için geçerli olması gerektiği, özel sektör için de muvafakat verilmesinin sıkıntılı bir durum yaratabileceği, muvafakat düzenlemesinin neye göre yapıldığına dair bir soruya cevaben,

2531 sayılı Kanuna göre Devletin, kural olarak, iki yıl belirli yerlerde çalışan kişilerin özel sektöre geçmesini yasakladığı, vergi incelemeleri nezdinde bir kamu görevlisinin üç yıl içinde incelediği şirkete veya kişiye geçemeyeceği, yoksa genel kuralın burada da geçtiği gibi iki yıl olduğu,

Belki çok nitelikli bir siber güvenlik uzmanının yine birçok özel şirketimizde -özel hukuk hükümlerine tabi TUSAŞ gibi, Mersin Nükleer Santrali gibi- çalışması gerektiğinde bu hükümlerin uygulanacağı, buna da ihtiyacımız olduğu, böyle bir yetkiyi Kurul başkanına vermenin ülkeye faydası olacağı, dile getirilmiştir.

15'inci madde üzerinde yapılan görüşmelerde,

Burada özellikle "Özel sektörün ekipmanlarını bedelsiz devralabilir." ifadesinin rahatsız edici ve sıkıntı doğurabilecek bir ifade olduğu, bedelsiz devralmanın şartları nasıl olacağı şeklindeki soruya cevaben,

Bir suç eşyasına yargılamada el koyma sürecinde, müsadere edilme üzerinden savcılığın talepte bulunacağı, bu süreçte el konulduğu, eğer bunun suç eşyası olduğu mahkemece karara bağlanırsa, kesinleşmekle birlikte müsadere edildiği ve mülkiyetinin devlete geçtiği, Devletin özel sektörün suç eşyasına da ücretsiz olarak el koyabileceği belirtilmiştir.

16'ncı madde üzerinde yapılan görüşmelerde,

Siber Güvenlik Kanunu Teklifi olarak Komisyona getirilen bu kanun teklifinin 16'ncı maddesinin, hukuk sistemimizde bugüne kadar var olmayan yeni suç ve cezalar ihdas ettiği, cezai düzenlemeler içeren bu kanunun Adalet Komisyonu tarafından incelenmesi ve değerlendirilmesi gerektiği,

Maddenin içerdiği yetkilendirmelerin Anayasa'nm 20'nci maddesinde güvence altına alınan özel hayatın gizliliği ve 22'nci maddesinde düzenlenen haberleşme hürriyetiyle açık bir çelişki içinde olduğu, Anayasa'nm 26'ncı maddesinde güvence altına alman ifade özgürlüğü ve 28'inci maddesinde korunan basın özgürlüğüyle bağdaşmadığı,

"Siber uzaydaki millî güç unsurları" gibi hukuki olarak tanımlanmamış ve sınırları belirsiz kavramlara ağır cezalar öngören Maddenin, Anayasa'nm 13'üncü ve 38'inci maddelerinde düzenlenen suç ve cezada belirlilik ilkesine aykırılık teşkil ettiği,

Suç ve cezanın belirsiz bir zemine oturtulmasının hem hukuki güvenlik ilkesini zayıflattığı hem de bireylerin hangi fiillerinin suç teşkil edeceğinin öngörülmesini imkânsız hâle getirdiği,

Ceza hukuku temel ilkeleri bağlamında ele alındığında 16'ncı maddenin birinci fıkrasının bir ceza kanunu olarak hapis cezası ve adli para cezasıyla cezalandırılmasının evrensel ceza hukuku ilkelerine aykırı olduğu, idari bir yaptırım veya kabahat niteliğinde olan bir eylemin cezai yaptırıma tabi kılınmasının Anayasa'ya aykırılık teşkil ettiği,

Teklifin 16'ncı maddesinin beşinci fıkrasının gazetecilik faaliyetlerini doğrudan hedef aldığı, daha önceki tarihlerde sansür yasası, dezenformasyon yasası gibi yasalarla belli bir ölçüde budanan basın ve ifade özgürlüğünün, geçtiğimiz aylarda etki ajanlığı yasası tartışmalarıyla yeniden ülke gündemine getirildiği, kamuoyundaki büyük tepkiler ve itirazlar sonucu geri çekilen bu yasanın Siber Güvenlik Başkanlığı Kanunu'nun satır aralarında yeniden karşımıza çıkarıldığı, bunun da devlet aklının özgürlükleri kısıtlamadaki ısrarını ve politikalarını gösterdiği,

Teklifin altıncı fıkrasının Türkiye Cumhuriyetinin siber uzaydaki millî gücünü oluşturan unsurlara yönelik saldırılara ağır cezalar öngördüğü, düzenlemenin millî güvenliği koruma amacı taşıyor gibi görünse de "siber uzaydaki millî güç unsurları" ifadesinin hukuki olarak tanımlanmamış olmasının ciddi bir belirsizlik yarattığı,

Cezaların sekiz ila on beş yıl gibi yüksek miktarlarda belirlenmesinin bu tür suçların niteliğiyle orantılı olmayan bir cezalandırma anlayışı sergilediği ve adil yargılanma hakkını ve hukuki güvenlik ilkesini zedeleme riski taşıdığı,

Siber güvenlik önlemleri alınırken birey hakları, basın özgürlüğü ve haber alma hakkının nasıl bir dengeye oturtulacağı,

Bir yandan toplumun ve devletin dijital güvenliğini sağlama yükümlülüğü diğer yandan Anayasa'nın 26'ncı maddesiyle korunan ifade özgürlüğünü güvence altına yükümlülüğü olduğunu ancak Siber Güvenlik Kanunu Teklifi'nin 16'ncı maddesinin bu dengeyi bozacak ve gazetecilik mesleğini ciddi bir tehdit altına sokacak düzenlemeler içerdiği şeklindeki görüş ve itirazlara cevaben,

Teklifin amacının veri sızıntılarını önlemek ya da en aza indirmek olduğu, bir kanunun geçerliliği ve uygulanabilirliğinin onun müeyyideleriyle bir bütün olduğu, aksi takdirde hukuktaki adıyla "ölü kanun" doğmuş olacağı,

Türk Ceza Kanunu'nun 217/A maddesi ile bunun arasında fark bulunduğu, orada bir bilginin dezenformasyon maksadıyla yayılmasının düzenlendiği, burada siber uzaydaki bir saldırı sonrası veri sızıntısı olduğu iddiasıyla korku, endişe ve panik yaratmanın zaten 2005 yılında yürürlüğe giren Ceza Kanunu'muzda o günden beri olduğu ve yeni bir kavram olmadığı,

Birçok kavramın içinin Yargıtay içtihatlarıyla doldurulduğu, Anayasa'mızın 39'uncu maddesinde ispat hakkı bulunduğu, bir kamu görevlisine karşı suç isnat eden kişinin, hakaret suçlarında ispatı kullanacağı, diğer suçlarda da kamunun bir menfaati varsa ispat hakkını kullanacağı,

Bir gazeteci sızıntı olduğunu iddia eder ve bunu ispatlarsa Anayasa gereğince hiç kimsenin bir şey diyemeyeceğini ancak sızıntı olmadığı hâlde kamuya ve borsaya açık, küçük yatırımcıların hisse aldığı bir yerde "Burada veri sızıntısı oldu, bütün bilgiler ele geçirildi, şirket batıyor." diye yayın yapıldığında buna müeyyide getirilmesi gerektiği ifade edilmiştir.

19'uncu madde üzerinde herhangi bir görüşme yapılmamış olmakla birlikte Maddede geçen "27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararnamenin ek 34'üncü maddesinin üçüncü fıkrasına aşağıdaki cümle eklenmiştir." ibaresine istinaden bu fıkra için,

"Anayasa Mahkemesinin 7/12/2023 tarihli ve E.:2018/117; K.:2023/212 sayılı Kararı ile bu fıkra iptal edilmiştir. Kararın Resmî Gazete'de yayımlanmasından başlayarak on iki ay sonra (4/6/2025) yürürlüğe gireceği hüküm altına alınmıştır."

bilgisine yer verilmiştir.

5. Teklif Metnine İlişkin Kabuller ve Değişiklikler

Teklifin tümü üzerinde yapılan görüşmelerin tamamlanmasının ardından, maddeleri üzerinde görüşmelere geçilmesi kabul edilmiştir.

Kanun Teklifinin;

1'inci maddesi kabul edilen önerge doğrultusunda metinde geçen "Türkiye Cumhuriyetinin" ibaresi "Türkiye Cumhuriyeti'nin" şeklinde değiştirilmesi suretiyle,

2’nci maddesi kabul edilen önerge doğrultusunda ikinci fıkrasının “4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanunu, 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet 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 uyarınca yürütülen faaliyetler bu Kanun kapsamı dışındadır” şeklinde değiştirilmesi ve Komisyonda redaksiyona tabi tutulmak suretiyle kabul edilmiştir. Teklif metnindeki “Salahiyet” ibaresi mevcut Kanunda yazıldığı “Salâhiyet” şeklinde düzeltilmiştir.

3’üncü maddesi aynen,

4’üncü maddesi Komisyonda redaksiyona tabi tutulmak suretiyle kabul edilmiştir. Teklif metnindeki “tedbirlerinin” ibaresinden sonra gelen “,” işareti çıkarılmıştır.

5, 6 ve 7’nci maddeleri aynen,

8’inci maddesi, kabul edilen önerge doğrultusunda gecikmesinde sakınca bulunan hallerde arama ve el koyma yetkisinin Cumhuriyet savcısına da tanınması ve bu işlemlerin “milli güvenlik, kamu düzeni, suç işlenmesinin veya siber saldırıların önlenmesi” amacıyla gerçekleştirilebilmesini ve bu işlemlerin makul sebeplerle yapıldığının gerekçelendirilmesine yönelik ibarelerin eklenmesi suretiyle değiştirilmesi suretiyle ve Komisyonda redaksiyona tabi tutulmak suretiyle kabul edilmiştir. Maddenin ikinci fıkrasının son cümlesindeki “görüldüğü” ibaresi anlatım bozukluğunun giderilmesi amacıyla “görülen” şeklinde ve beşinci fıkrasında yer alan “elkoyma” ibareleri Türk Dil Kurumu kullanımına uygun olarak “el koyma” şeklinde değiştirilmiştir.

9, 10, 11’inci maddeleri aynen,

12’nci maddesi Komisyonda redaksiyona tabi tutulmak suretiyle kabul edilmiştir. Tanımlar maddesinde “Siber Güvenlik Başkanlığı” zaten tanımlandığından madde metnindeki “Siber Güvenlik Başkanlığınca” ibaresi “Başkanlıkça” şeklinde değiştirilmiştir.

13’üncü maddesi aynen,

14’üncü maddesi Komisyonda redaksiyona tabi tutulmak suretiyle kabul edilmiştir. Maddenin (a) bendinde yer alan “hazine” ibaresi “Hazine” şeklinde değiştirilmiştir.

15’inci maddesi aynen,

16’ncı maddesinin beşinci fıkrası, kabul edilen önerge doğrultusunda “(5) Siber uzayda veri sızıntısı olmadığı halde halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef almak amacıyla veri sızıntısı yapılmış gibi içerik oluşturanlara ve/veya bu içerikleri yayanlara iki yıldan beş yıla kadar hapis cezası verilir.” şeklinde değiştirilmek suretiyle,

17, 18, 19, Geçici 1’inci, 20 ve 21’inci maddeleri aynen,

oy çokluğuyla kabul edilmiştir.

Kanun Teklifinin maddeleri üzerindeki görüşmelerin tamamlanmasının ardından, tümü oya sunulmuş ve oy çokluğuyla kabul edilmiştir. Kanunların hazırlanmasında uygulanan esas ve usuller çerçevesinde, Kanun Teklifinde anlatımın açıklığa kavuşturulması ve kanun tekniğine uygunluğun sağlanması amacıyla Komisyon Başkanlık Divanına redaksiyon yetkisi verilmesi hususu oya sunulmuş ve kabul edilmiştir. Bu çerçevede Kanun Teklifinin tamamı gözden geçirilmiş ve metinde redaksiyon mahiyetinde değişiklikler yapılmıştır.

6. Genel Kurulda Temsil

İçtüzüğün 45'inci maddesi uyarınca, Teklifin Genel Kuruldaki görüşmelerinde Komisyonumuzu temsil etmek üzere İzmir Milletvekili Mehmet Ali Çelebi, Bingöl Milletvekili Feyzi Berdibek, Şanlıurfa Milletvekili Mehmet Ali Cevheri, Ordu Milletvekili İbrahim Ufuk Kaynak ve Antalya Milletvekili İbrahim Ethem Taş, Teklif ile ilgili özel sözcü seçilmişlerdir.

Başkan	Başkanvekili	Sözcü
Hulusi Akar	*Refik Özen*	*Zuhal Karakoç Dora*
Kayseri	Bursa	Kahramanmaraş
Kâtip	Üye	Üye
Mehmet Ali Çelebi	*Ayyüce Türkeş Taş*	*İbrahim Ethem Taş*
İzmir	Adana	Antalya
(Bu raporun özel sözcüsüdür)	(Muhalefet şerhimiz vardır)	(Bu raporun özel sözcüsüdür)
Üye	Üye	Üye
Feyzi Berdibek	*Ayhan Salman*	*Özgür Ceylan*
Bingöl	Bursa	Çanakkale
(Bu raporun özel sözcüsüdür)		(Muhalefet şerhimiz vardır)
Üye	Üye	Üye
Onur Düşünmez	*Vezir Coşkun Parlak*	*Adnan Şefik Çirkin*
Hakkâri	Hakkâri	Hatay
(Muhalefet şerhimiz vardır)	(Muhalefet şerhimiz vardır)	(Muhalefet şerhimiz vardır)
Üye	Üye	Üye
Mehmet Uğur Gökgöz	*Aşkın Genç*	*Metin İlhan*
Isparta	Kayseri	Kırşehir
	(Muhalefet şerhimiz vardır)	(Muhalefet şerhimiz vardır)
Üye	Üye	Üye
Abdullah Ağralı	*Konur Alp Koçak*	*İbrahim Ufuk Kaynak*
Konya	Konya	Ordu
		(Bu raporun özel sözcüsüdür)
Üye	Üye	Üye
Seyit Torun	*Mehmet Ali Cevheri*	*Abdürrahim Dusak*
Ordu	Şanlıurfa	Şanlıurfa
(Muhalefet şerhimiz vardır)	(Bu raporun özel sözcüsüdür)	
	Üye	
	Eylem Ertuğ Ertuğrul	
	Zonguldak	
	(Muhalefet şerhimiz vardır)	

MUHALEFET ŞERHİ

1. GENEL DEĞERLENDİRME

24 Haziran 2018 tarihli seçimlerinin ardından 9 Temmuz 2018 tarihinde geçiş yapılan, adına 'Cumhurbaşkanlığı Hükümet Sistemi' denilen ve sürecin başından itibaren dile getirdiğimiz yeni hükümet sisteminin bir 'tek adam' rejimi olduğu yönünde ileri sürdüğümüz görüşlerin ne kadar yerinde olduğu görüşülen (2/2860) esas numaralı tekliften de anlaşılmaktadır.

Söz konusu kanun teklifi 10 Ocak 2025 tarihinde Türkiye Büyük Millet Meclisi Başkanlığına verilmiş, aynı tarihte esas komisyon olarak Milli Savunma Komisyonuna tali komisyon olarak Adalet, Plan ve Bütçe ile Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonlarına sevk edilmiştir.

Söz konusu kanun teklifinin 15 Ocak 2025 günü saat 13.30'da Milli Savunma Komisyonunun yapacağı toplantının gündemine alındığı, Komisyon Başkanlığının 13.01.2025 tarih ve Z-19673998-130.02-1563947 sayılı yazıları ile komisyon üyelerine bildirilmiştir.

9 Temmuz 2018 sonrasında TBMM'de görüşülen tekliflerin kahir ekseriyetinde olduğu gibi bu teklifte 'Saray mutfağında' hazırlanmış, usul hukuku gereği imzaları tamamlanarak TBMM Başkanlığına sevk edilmiş ve başkanlıkça da gündeme alınmış intibası uyandırmaktadır. Ülkeyi yöneten tek adamın kervan yolda düzülür anlayışıyla hareket etmesindendir ki (2/2860) esas numaralı **Siber Güvenlik Kanunu Teklifi'ne** ihtiyaç duyulmuştur. Söz konusu teklif henüz TBMM Başkanlığına verilmeden iki gün önce 08 Ocak 2025 Tarih ve 32776 Sayılı Resmî Gazetede yayınlanan 177 Sayılı Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi ile Merkezi Ankara'da bulunan kamu tüzel kişiliğine haiz Cumhurbaşkanlığı'na bağlı "Siber Güvenlik Başkanlığı" kurulduğunu öğreniyoruz. Tesadüfe bakın ki 10 Ocak 2025 tarihinde de Siber Güvenlik Kanun Teklifi TBMM Başkanlığına sunuluyor.

Şöyle ki teklif sahibi Afyonkarahisar Milletvekili Sayın Ali Özkaya komisyonda yaptığı konuşmada "Geçen yıl, bir önceki yıl yaptığımız TCK 217/A'daki suç yani halkı belirli bir şekilde yönlendirmeye matuf ve sosyal medyadaki algı ve dezenformasyon oluşturma suçunun kapsamı, suçun unsurları çok ağır, kapsamı çok dar. Bugünkü sosyal medya ve dünyadaki dijitalin geldiği noktada bu mevcut suç bu amacı karşılamıyor. Dolayısıyla, burada bir değişikliğe ve yeni bir ilave hükme ihtiyaç olduğu kanaati var.

Cumhurbaşkanlığı Dijital Ofisimiz tarafından yapılan çalışmalarda dünya ülkelerinin çok büyük kısmında merkezî bir otoritenin kurulduğunu, merkezî otoritenin standardizasyonu, sertifikasyonu ve denetlemeyi yaptığını görüyoruz. Bunların bizim ülkemize de getirilmesiyle birlikte bu alandaki kamusal açıklarımızın ciddi manada önleneceğini düşünüyoruz" ifadelerini kullanarak teklifin nerede hazırlandığını kendisi de belirtmiş oldu.

Yine teklifin genel gerekçesinde; "Ülkemizdeki siber güvenlik yapılanmasında Ulaştırma ve Altyapı Bakanlığı, Sanayi ve Teknoloji Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi başta olmak üzere birçok kamu kurumunun sorumlulukları bulunmaktadır" ifadeleri yer almaktadır. En azından gerekçede sorumlulukları açıkça ifade edilen bakanlıkların faaliyetlerine ilişkin TBMM'nin ilgili alanlardaki ihtisas komisyonlarından Dijital Mecralar Komisyonu ile Bayındırlık, İmar, Ulaştırma ve Turizm Komisyonuna da teklif tali olarak dahi sevk edilebilirdi. Bu sevkin yapılması sürece olumlu bir katkı yapar mıydı? 9 Temmuz 2018 sonrası hakim olan anlayışın pratiğinde bu pek mümkün görünmüyor.

Zira söz konusu kanun teklifinin sevk edildiği Adalet, Plan ve Bütçe ile Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonlarında da gündeme alınıp görüşülmeyeceğinin bildirildiğini sayın komisyon başkanı ifade etmiştir. TBMM'de ilgili ihtisas komisyonlarında yeterince tartışılıp görüşülmeden acele bir şekilde geçen çok sayıda yasanın kısa süre içinde defalarca değiştirildiğine tanıklık ediyoruz. (2/2860) esas numaralı Siber Güvenlik Kanunu Teklifi'de benzer bir akıbeti yaşayacak, muhtemelen genel kurulda da parmak demokrasisi marifetiyle geçecek ve Anayasaya aykırılıklarıyla, özgürlüklere keyfi olarak müdahale edebilmenin önünü açan düzenlemeleriyle yasalaşacak.

Bir tek adam dönemi yasa yapma geleneği halini alan tali komisyonların kendilerine sevk edilen kanun teklifleri üzerinde inceleme yapmama hali bu teklifte de tezahür etmiştir.

Komisyonda 1'inci madde üzerinde verdiğimiz önerge kabul edilmiş ve 2'inci madde üzerinde verdiğimiz önerge ile aynı mahiyetteki Ak Parti önergesi kabul edilmiştir. Komisyonumuz uzmanlık alanıyla hiç ilgisi olmayan ceza hukuku ile ilgili maddelere ilişkin eleştirilerimiz, ilgili ihtisas komisyonlarında görüşülmesine ilişkin önerilerimiz kabul görmemiş, parmak çoğunluğuyla ilgili maddeler geçmiştir. 8'inci ve 16'ıncı maddelerde Ak Parti önergeleri ile bir değişiklik yapılmışsa da arzu edilen Anayasa'ya aykırılık iddiamızı bertaraf eder mahiyette değildir.

Modern toplumların demokratik gelişmişlik düzeyinin en önemli belirleyici unsurlarından biri de şüphesiz halkın siyasi ve idari karar alma süreçlerine katılım mekanizmalarının işleyip işlemediğidir. Demokratik ve ekonomik açıdan gelişmiş birçok ülke bunu güçlü sivil toplum örgütlerine ve işleyen Adalet ve hukuk mekanizmasına borçludur. Buda uluslararası finansal hareketler bakımından cazibe yaratmakta, bu ülkelerin yurttaşları refah içinde yaşarlarken devletler de ulusal çıkarlarını çok daha etkin ve güçlü bir şekilde savunabilmektedir.

2022 yılında Economist Intelligence Unit (EIU) tarafından yapılan Demokrasi Endeksi çalışmasında Türkiye, 167 ülke arasından 103'üncü sırada kendine yer bulabildi. 10 üzerinden yapılan değerlendirmede Norveç, 9,81puan ile listenin zirvesinde, Afganistan 0,32 puanla son sırada yer aldı. Sürdürülebilir Kalkınma Amaçlarının olmazsa olmazlarından biri olarak kabul edilen demokrasi hedefi, 2023 yılında da arzu edilen sıçramayı yapamadı ve bir basamak yükselerek 4.33 puan ile sıralamada 102'nci oldu. Endeskte ülkeler, 'tam demokrasi', 'kusurlu demokrasi', 'hibrit (karışık/melez) rejim' ve 'otoriter rejim' olarak dört ana kategoride değerlendirilirken ülkemizin "hibrit demokrasi" kategorisinde kıymetlendirilmesi şaşırtıcı olmasa da üzüntü verici bir durum olarak kayda geçmiştir.

İfade özgürlüğü, Anayasamız ve kanunlarımızla güvence altına alındığı gibi, Evrensel İnsan Hakları Bildirgesi'nin 19. Maddesi'nde de güvence altına alınmış temel bir insan hakkıdır. Ancak dünya genelinde, geri bırakılmış birçok ülke hükümetleri otoriter yönetim anlayışları gereği ifade özgürlüğünü ve demokrasiyi hiçe sayma eğilimi sergiliyor.

Teklifin mevcut haliyle yasalaşması durumunda Türkiye'nin demokratik değerlerindeki aşınmanın artarak devam edeceğini söylemek yerinde olacaktır. Hızla demokratik toplum düzenine ve temel insan haklarına yabancılaşmaya başlayan sistem, Yunanistan'ın 'Tam demokrasi' kategorisine geçmeyi başardığı bir süreçte, belki de 2025 -2026 yıllarında 'hibrit demokrasi' kategorisinden 'otoriter rejim' kategorisine gerileyecektir ki buda içinde bulunduğumuz ekonomik krizin biraz daha derinleşmesi anlamında etkili olacaktır.

Birçok Avrupa ülkesi, ulusal düzeyde siber güvenlik stratejileri geliştirmiş ve bu alanda yetkili kurumlar oluşturmuştur. Almanya, Fransa, Birleşik Krallık ve Hollanda gibi ülkeler, kapsamlı ve entegre yaklaşımlarıyla öne çıkmaktadır.

Siber güvenlik politikalarının amacı, dijital ortamın güvenliğini artırarak ifade özgürlüğü de dahil olmak üzere temel hakların korunmasına katkıda bulunmak olmalıdır. İfade özgürlüğünü sınırlandırma riski taşıyabilecek düzenlemelerden ve belirsizliklerden kaçınmak esas olmalıdır.

Bireylerin haklarını ihlal etmeyen ancak aynı zamanda güvenliği de sağlayan bir yaklaşımın zorunlu olduğu siber güvenlik alanına ilişkin yapılacak düzenlemelerde ifade özgürlüğü ve kişisel verilerin gizliliği gibi bir birleri arasında hassas bir denge bulunan ve en temel insan haklarından olan bu alanlarda söz konusu hakları ihlal etmeden hareket edebilmek için Avrupa Birliği'nin bu alandaki yasal çerçeveleri ve kurumlarının incelenerek örnek alınması bu anlamda en azından AB standartlarının sağlanabilmesi yerinde olabilir.

Teklifin hazırlık safhasında basın meslek örgütleri ve sivil toplum örgütleri ile bir araya gelinip, onların görüşleri alınmamıştır. Teklifin komisyon görüşmelerinde de basın meslek örgütleri adına teklife ilişkin eleştirisi olabilecek çağrılı kimse olmadığı gibi STK temsilcileri de yoktu. Türkiye Odalar Ve Borsalar Birliği Türkiye Yazılım Meclisi Başkanı Ertan Barut'a şeklen söz verilmiş, Sayın Barut'ta iki dakikalık konuşmasında selamlama, kendinden bahsetme ve teşekkür faslı dahil olmak üzere toplam 243 kelime kullanmıştır. Komisyon'da Türkiye Odalar Ve Borsalar Birliği Türkiye Yazılım Meclisi'nin bu teklife ilişkin görüşleri anlaşılamamıştır.

Siber Güvenlik Kanun Teklifine ilişkin olarak en kapsamlı izleme ve değerlendirme de bulunan sivil toplum örgütü 'İfade Özgürlüğü Derneği' olmuştur.

MADDELERE İLİŞKİN GÖRÜŞLERİMİZ

Teklif, belirsiz kavramlar getirerek, kurulacak Siber Güvenlik Başkanlığı'na aşırı geniş ve denetimsiz yetkiler tanımakta, bu yetkilerin kullanımı kapsamında kişi ve kuruluşlara orantısız adli ve idari yaptırımlar öngörmektedir. Teklifin içeriğine bir bütün olarak baktığımızda metnin ruhunun ifade ve basın özgürlüğü başta olmak üzere, özel hayatın gizliliği,

kişisel verilerin korunması gibi temel hak ve özgürlüklerin korunması açısından büyük risk ve tehditler barındırdığı görünmekte. Siber tehdit, siber olay, veri sızıntısı, algı operasyonu gibi muğlak, belirsiz ifadelerle keyfî uygulama ve yaptırımlara açık bir düzenlemeyle karşı karşıya olduğumuzu kıymetlendiriyoruz.

Bu muğlak ifadeler en başta demokratik toplumların temel değerlerinden biri olan öngörülebilirlik ve hukuki güvence ilkelerine aykırıdır. Dolayısıyla Anayasa'mızın 2'nci maddesinden, 6'ncı, 7'nci, 9'uncu, 11'inci, 13'üncü maddesi ve 26, 27 ila 28'inci maddeleri çerçevesinde basın özgürlüğü, temel hak ve özgürlüklerin korunması, belirlilik kavramları hukuk devleti ilkeleri açısından önemli nirengi noktalarıdır ve teklifin 5, 6, 8 ve 16'ncı maddelerinin bu manada Anayasaya aykırı olduğu kanaatindeyiz.

Yasa teklifinin 3'üncü maddesi ile Türk hukukunda daha önce tanımlanmamış olan "kritik altyapı", "kritik kamu hizmeti", "Siber Olay" gibi soyut kavramlar ilk kez kapsama alınmaktadır. Ancak, Yasada bu kavramların içeriği açık bir şekilde belirtilmemiş, teklifin 5. madde ile bu belirleme yetkisi doğrudan Başkanlığa bırakılmıştır. Anayasamızın 6'ıncı maddesi: "Hiçbir kimse veya organ kaynağını Anayasadan almayan bir Devlet yetkisi kullanamaz." Anayasa madde 6 kesin bir yasak getirmektedir.

Yasama organının yetkisi bakımından da Anayasa madde 7'ye göre tekelci, devredilemez bir yetki söz konusudur. Ancak bu yetki kullanılırken de göz önünde bulundurulması gereken husus Anayasa'nın 11'inci maddesidir. Şu halde "Kanunlar Anayasaya aykırı olamaz." hükmünü içeren, Anayasa'nın üstünlüğü ve bağlayıcılığı kuralını öngören Anayasa madde 11 çerçevesinde, anayasal bağlamda kullanılan bir yetkidir. Sınırsız bir yetkiden bahsedilemez. Bu anlamda "kanun" kavramı, yasama organın genellik ve soyutluk ilkesi çerçevesinde yerine getirmesi gereken bir işlemdir.

Dolayısıyla bu durum, yasama yetkisinin idareye devri anlamına gelmektedir ve Anayasaya açıkça aykırıdır. Ayrıca, kanunun genellik ve soyutluk niteliklerine aykırılığı sebebiyle de Anayasa'nın 2. maddesinde öngörülen hukuk devleti ilkesiyle uyumsuzluğundan bahsedilebilir.

Bu durum Başkanlığın keyfi olarak, özerk olması gereken üniversiteler, bağımsız idari otoriteler gibi kurumları kritik altyapı ilan etmesinin de önünü açacaktır. Böyle bir tanımlama, özerk olması gereken kurumların tüm faaliyetlerini Başkanlığın denetimi altına alabilir ve iş birliği yapmayanlara 16. madde uyarınca ağır yaptırımlar uygulanmasına neden olabilir.

Bir siyasetçi olan Cumhurbaşkanı'na kişisel bağlılığı ve biat etmesi üzerinden görev yapacak bir bürokrata bu denli geniş yetkiler verilmesi demokrasimiz açısından ciddi tehlikeler içermektedir.

Yasadaki belirsizlik, yalnızca bu kavramlarla da sınırlı değildir. Öngörülen kurumsal yapı da Anayasa'nın 123. maddesinde güvence altına alınan kanuni idare ilkesine aykırıdır. Bu maddeye göre kurulacak bir idarenin şeklen yasayla kurulmuş olması yeterli değildir, idarenin yapısının maddi olarak da Yasayla belirlenmesi gerekir. Anayasa Mahkemesi'nin belirttiği gibi "Anayasanın 123 üncü maddesinde yer alan idarenin kanuniliği ilkesi, yasamanın, bir alanı temel ilkeleriyle belirlemesi, düzenlemesi; ondan sonra da, yürütmenin, bu çerçevesi çizilmiş alanda düzenleyici birtakım işlemler yapabilmesini gerektirir. Anayasanın 7. maddesine göre

yasama yetkisi Türkiye Büyük Millet Meclisi'nindir ve bu yetki devredilemez." (AYM, E: 2011/149, K:2012/187, K.T.: 22.11.2012)

5. maddeye göre SOME'ler Başkanlık tarafından kurulup denetlenecektir. Bununla birlikte SOME'lerin kimlerden oluşacağı, yetkilerinin ne olduğu ve burada çalışacak kişilerin seçiminin nasıl yapılacağı belirsizdir. 6. madde, bu tür detayların Cumhurbaşkanlığı tarafından çıkarılacak bir yönetmelikle belirleneceğini ifade etmektedir. Ancak, yasanın kendisinin sınırlarını çizmediği bir konuda Cumhurbaşkanlığı yönetmeliğiyle düzenleme yapılması Anayasa'nın yasallık ilkesine aykırıdır. Bu belirsizlikler, yalnızca hukuki öngörülebilirliği zedelemekle kalmamakta, aynı zamanda bireylerin haklarını keyfi müdahalelere karşı savunmasız bırakmaktadır. Yasa kapsamındaki soyut ve belirsiz yetkiler, temel hak ve özgürlüklerin kısıtlanmasını sağlayabilir.

Teklif ile ihdas edilen suç ve cezalar da yasallık ilkesini ihlal etmektedir. Suç ve cezaların yasallığı ilkesinin ihlalinin doğrudan kişi özgürlüğünü kısıtlama potansiyeli nedeniyle daha da ağır sonuçları vardır. Teklifin 16. ve 17. maddelerinde yer alan ağır cezalar, yalnızca kişisel hakları değil, aynı zamanda temel anayasal güvenceleri de tehdit etmektedir.

Anayasa Mahkemesinin bir çok kararında ifade ettiği gibi suç ve cezaların kanuniliği ilkesi, genel olarak bütün hak ve özgürlüklerin düzenlenmesinde temel bir güvence oluşturmanın yanı sıra suç ve cezaların belirlenmesi bakımından özel bir anlam ve önem taşımakta; bu kapsamda kişilerin kanunen yasaklanmamış veya yaptırıma bağlanmamış fiillerden dolayı keyfî bir şekilde suçlanmaları ve cezalandırılmaları önlenmekte; buna ek olarak suçlanan kişinin lehine olan düzenlemelerin geriye etkili olarak uygulanması sağlanmaktadır (Karlis A.Ş., B. No: 2013/849,15/4/2014, § 32).

Özellikle yetki alanı tanımlanmamış denetim mercilerinin talimatlarına uymayan bireylerin cezalandırılmasını öngören maddeler, keyfi uygulamalara kapı aralamaktadır. Ayrıca, yasa kapsamında belirlenen cezaların ölçüsüzlüğü, hukuk devleti ilkesine aykırılık teşkil etmekte ve bireylerin temel haklarını ağır şekilde ihlal etme riski taşımaktadır.

Teklifin 6. maddesinde tanımlanan yetkiler, yasal güvenceden yoksun, keyfi uygulamalara yol açabilecek ve denetlenemeyen bir sistem öngörmektedir. Yasa teklifinin 6. maddesinin birinci paragrafının (b), (ç), ve (d) bentleri, Siber Güvenlik Başkanlığına sınırsız bir erişim yetkisi tanımaktadır. Buna göre Başkanlık, "her türlü bilgi, belge, veri ve log kayıtlarını" Başkanlık sistemlerine aktarabilir; elektronik bilgi işlem merkezlerinden, iletişim altyapılarından ve arşivlerden sınırsız şekilde faydalanabilir. Bu düzenlemelerde hakim onayı şartı aranmamaktadır ve yasal süreçlerin nasıl işleyeceği belirsiz bırakılmıştır. Bu durum, bireylerin özel hayatına keyfi bir müdahale riskini beraberinde getirmektedir ve Anayasanın 20'inci maddesine açıkça aykırılık teşkil etmektedir.

Hakim onayı olmaksızın bilgiye erişim yetkisi, sadece bireylerin mahremiyetini değil, aynı zamanda kişisel verilerin güvenliğini de tehdit etmektedir. Kanunun 6. maddesi, Başkanlığın hangi tür bilgilere erişim sağlayacağı konusunda herhangi bir sınır çizmemektedir. Özellikle, kişisel veri barındıran bilgi ve belgelerin alınması, işlenmesi ve saklanması konularında yasal güvence eksikliği dikkat çekicidir. Bu belirsizlik, kişisel verilerin tamamen keyfi şekilde erişilebilir hale gelmesine zemin hazırlamaktadır. Bu durum, yalnızca bireylerin

değil, aynı zamanda sivil toplum kuruluşları, basın kuruluşları ve özel sektör şirketlerinin de veri güvenliğini tehlikeye atmaktadır.

Teklifin 6 (1) (ç) maddesinde "elde edilen bilgi, belge, veri ve kayıtlar, en fazla iki yıl süreyle çalışmaya konu edilir ve çalışma süresi sonrasında imha edilir" ve 6(2) maddesinde de "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" denilmiştir. Fakat teklif edilen Yasa metninde Başkanlık tarafından elde edilecek bilgi ve belgelerle ilgili yasal güvenceler yer almamaktadır.

Anayasa'nın 13. ve 20. maddeleri uyarınca kişisel verilerden korunmasını isteme hakkını sınırlamaya yönelik kanuni bir düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli ve öngörülebilir düzenlemeler niteliğinde olması gerekir (AYM, E.: 2018/91 K.: 2020/10, 19.02.2020, 95) Anayasa Mahkemesi, 5651 Sayılı Kanun'da yer alan benzer yetkileri iptal etmiştir. Anayasa Mahkemesi bu kararlarında, belirli ve öngörülebilir olmayan düzenlemelerin kişisel verilerin korunması hakkını ölçüsüzce sınırlandırmakta olduğunu ve Anayasa'nın 20. maddesine aykırılık teşkil ettiğini tespit etmiştir.

Benzer bir durum teklif ile Siber Güvenlik Başkanlığına verilen yetkiler bakımından da söz konusudur. Başkanlığın tamamen keyfi olarak tüm işletmelerden temin edebileceği, talep edilecek olan bilgilerin mahiyetinin belirsiz olduğu ve kişisel verileri de içerecek nitelikteki her türlü bilgi ve belge nedeniyle zarar görecek kişilerin Başkanlığın bilinmeyen ve hakim onayı şartı aranmayan kararlarına karşı hukuki yollara başvurması, itiraz etmesi mümkün olmadığı gibi özel hayata müdahaleye sebep olacak bu uygulamanın hak arama hürriyetini ortadan kaldırmasının ötesinde, Anayasanın 40. Maddesi ve Avrupa İnsan Hakları Sözleşmesi'nin 13. Maddesinde öngörülen etkili başvuru yolunu kullanılamaz hale getireceği açıktır.

Teklif, Başkanlığa geniş yetkiler tanımasına rağmen bu yetkilerin kullanımıyla ilgili herhangi bir bağımsız denetim mekanizması öngörmemektedir. Başkanlığın keyfi işlemleriyle zarar görecek bireyler için etkili bir denetim veya başvuru mekanizması da bulunmamaktadır. Bu eksiklik, teklifin temel hak ve özgürlükleri koruma konusundaki güvenilirliğini tamamen ortadan kaldırmaktadır.

Açıklamak gerekirse, Başkanlığa teslim edilecek kişisel bilgi ve verilerin "iki yıl sonra" imha edileceği belirtilmiş olmasına rağmen teklifte imha edilip, edilmeyeceği hususunda herhangi bir yasal güvence belirtilmemiştir. Bu konuda ihmali veya kusuru olanlar ve dolayısıyla Başkanlık personeli açısından herhangi bir ceza veya yaptırım öngörülmemiş, Başkanlığın da bağımsız bir şekilde denetlenmesi de Yasa teklifinde öngörülmemiştir. Bu hususun yargısal denetimi de neredeyse imkansızdır.

Teklif edilen Yasanın 16. maddenin 5. fıkrası, komisyonda AK Parti önerisi doğrultusunda *"Siber uzayda veri sızıntısı olmadığı halde halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef almak amacıyla veri sızıntısı yapılmış gibi içerik oluşturanlara ve/veya bu içerikleri yayanlara iki yıldan beş yıla kadar hapis cezası verilir"* şeklinde değiştirilmiştir. Ancak bu değişiklik, teklifte geçen "algı oluşturmak" ifadesini çıkararak önerge gerekçesindeki ifadeyle "metinde geçen atıf ve tanımların daha açık ve net bir

şekilde tanımlanması amaçlanmaktadır" dese de Türk Ceza Kanunu'nun 217/A maddesindeki "Halkı yanıltıcı bilgiyi alenen yayma suçu" ve yasalaşmayan "etki ajanlığı" suçlarıyla benzer sorunları yeniden gündeme taşımaktadır.

Madde metninde yer alan "Veri sızıntısı olmadığı halde" ifadesinin fiiliyatta ne şekilde tespit edileceği açıklanmamıştır. Bu durumun tespiti amacıyla bir mahkeme kararının mevcudiyeti yahut bilirkişi incelemesi veya veri sızıntısının olup olmadığını objektif bir biçimde ortaya koyabilecek bir test sonucunun esas alınması gerekmektedir.

Öte yandan, bu hususta yapılan bir açıklamanın etkinliği/ağırlığı tespit edilmeksizin, kurumsal/bireysel açıklama ayrımı yapılmaksızın yalnızca "hedef almaya yönelik faaliyet yürütenler" şeklinde ifade edilmesi de hatalıdır. Zira sade vatandaşlar ya da sosyal medya kullanıcıları bu noktada verilerinin çalındığını düşünse dahi düşünce açıklamasında bulunamayacak ve bu bir otosansür yöntemine dönüşecektir. Dolayısıyla bu hususta fiilin ağırlığını ortaya koyacak, söz konusu açıklamanın etki alanını belirleyecek objektif kriterler ortaya konulmalıdır.

Söz konusu maddelerin ifade özgürlüğü, basın özgürlüğü, özel hayatın gizliliği ve kişisel verilerin korunması açısından ciddi sorunlar yaratabileceği hususunda genel bir algı bulunmaktadır. Özellikle veri sızıntısı olmadığı hâlde veri sızıntısı yapılmış gibi açıklama yapan ve bu suçu işleyenlere 2-5 yıl arasında hapis cezasının öngörülmesi basın özgürlüğüne yönelik sistematik bir tehdit olarak karşımıza çıkmaktadır.

Teklifin 6'ncı maddesiyle Siber Güvenlik Başkanlığına kamu kurumları ve kritik altyapı kuruluşlarından veri ve Log kayıtlarını toplama, iki yıl süreyle saklama ve çalışma süresi sonunda imha yetkisi öngörülüyor. Peki, bu veriler nasıl korunacak, hangi koşullarda imha edilecek, kişisel verilerin kötüye kullanımının önüne nasıl geçilecek; ortada büyük bir belirsizlik vardır. Gazeteciler için haber kaynaklarından alınan veriler, belgeler, kayıtlar nasıl korunacak bilinmemektedir. Bu düzenleme sadece gazetecilik için değil, özel hayatın gizliliği ve demokratik denetim için de oldukça kaygı vericidir.

Bu tür belirsiz ve geniş tanımlamalar, ifade özgürlüğünü doğrudan tehdit etmekle kalmayıp bireylerin ve kurumların eleştiri yapma cesaretini de kırmaktadır. Özellikle gazeteciler, sivil toplum kuruluşları ve insan hakları savunucuları gibi toplumun demokratik denetim işlevini yerine getiren gruplar üzerinde caydırıcı bir etki yaratacağı açıktır. Eleştirel görüşlerin ve kamuyu bilgilendirme hakkının keyfi cezalandırılma riskiyle karşı karşıya kalması, bu düzenlemeyi demokratik bir hukuk devleti anlayışıyla bağdaştırmayı imkânsız hale getirmektedir. Bu bağlamda, siber güvenlikle ilgili kamuoyunu yakından ilgilendiren veri sızıntısı veya veri ihlali iddiaları ve paylaşımları hedef alınabilir, bireylerin özgürce ifade hakkını kullanmaları engellenebilir ve veri ihlali iddialarını bildiren kişiler ağır cezalar öngören bu suçtan yargılanabilir.

Teklifin 8'inci maddesinin (5)'inci fıkrasıyla Siber Güvenlik Başkanlığına gecikmesinde sakınca bulunan hâllerde hâkim onayı olmaksızın arama yapma, dijital materyallere el koyma ve veri toplama yetkisi tanınmaktadır. Bu düzenleme de özellikle araştırmacı gazetecilik için büyük tehdit oluşturmaktadır. Gazetecilerin haber kaynağından aldığı belgeler, iletişim kayıtları bu yetki kapsamında erişilebilir hâle gelecektir ki bu durum kabul edilemezdir.

"Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi veya siber saldırıların önlenmesi amacıyla Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet Savcısının veya Başkanın yazılı emri ile konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama yapılabilir ve kopya çıkarma ve elkoyma işlemi gerçekleştirilebilir. Hâkim kararı olmaksızın yapılan arama ve gerçekleştirilen kopya çıkarma ve elkoyma 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 elkoyma kendiliğinden kalkar. Bu fıkra kapsamına giren talepler bakımından Ankara sulh ceza hâkimliği yetkili ve görevlidir. Ancak kamu kurum ve kuruluşları bakımından hâkimlik kararı aranmaz."

1. "Başkanın yazılı emri" ile arama/elkoyma işlemi yapılabilmesi sakıncalıdır. Siber Güvenlik Başkanı'nın, yargı organının yerine geçerek arama ve elkoyma kararı vermesi mümkün değildir.
2. Maddede bahsi geçen "gecikmesinde sakınca bulunan haller" ibaresi keyfi tutumlara yol açabilecek, muğlak, belirsiz bir ifadedir.
3. "Başkanın emriyle yapılan işlemler daha sonradan hâkimin onayına sunulacaktır." hükmü, durumun hukuksuz oluşunu ortadan kaldırmamakta, neticeten başkanın hiçbir şarta bağlı kalmaksızın vereceği bir karar vasıtasıyla konut dokunulmazlığı dahil birçok kişi hak ve özgürlüğüne müdahale edilebilecek, kişilerin huzur ve sükununa dokunulabilecektir. Söz konusu işlemlerin yalnızca hâkim kararıyla yapılması gerekmektedir.
4. Arama kararının içeriğinin neye göre belirleneceği, arama kararının karşılaması gereken kriterlerin neler olduğu açıklanmamıştır.

5271 Sayılı Ceza Muhakemesi Kanununun 119/2 maddesi örnek alınacak olursa, kararın taşıması gereken nitelikler aşağıdaki şekilde belirlenebilir.

Arama karar veya emrinde;

-Aramanın nedenini oluşturan fiil

-Aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya,

-Karar veya emrin geçerli olacağı zaman süresi, açıkça gösterilmelidir.

Aksi halde; neye ilişkin olduğu, ne sebeple yapıldığı, nerede yapılacağı belirtilmeyen bir arama/el koyma kararı, ölçülülük ve belirlilik ilkesine aykırılık teşkil edecektir.

Dolayısıyla bütün bu gerekçelerden ötürü teklifin 3, 5, 6, 8 ve 16'ncı maddelerinin ifade özgürlüğü, basın özgürlüğü, özel hayatın gizliliği ve kişisel verilerin korunması açısından ciddi sorunlar yaratacağını ve Anayasanın 2, 7, 8, 9, 11, 13, 20, 21, 25, 26 ve 28'inci maddelerine açıkça aykırı olduğunu kıymetlendiriyoruz.

Özgür Ceylan	*Seyit Torun*	*Eylem Ertuğ Ertuğrul*
Çanakkale	Ordu	Zonguldak
Metin İlhan		*Aşkın Genç*
Kırşehir		Kayseri

MUHALEFET ŞERHİ

"BÜYÜK BİRADER SENİ İZLİYOR!"

"Cihan Bilgin ve Nazım Daştan'ın Anısına Saygıyla…"

GENEL DEĞERLENDİRME

20. yüzyılın ortalarından itibaren gelişmekte olan bilgisayar teknolojileri, yüzyılın sonuna doğru yoğun bir ivme kazanmış ve hayatın her alanında etkisini gösterir hale gelmiştir. Günümüzde ulaşımdan iletişime, eğitimden bürokrasiye, endüstriden savunmaya kadar birçok alanı bilgisayar teknolojilerinden bağımsız ele almak mümkün değildir. Bilgisayar teknolojisi, sözü edilen alanların yanı sıra gündelik hayatta da bilgisayarlar, telefonlar, giyilebilir teknolojiler vb. aracılığıyla insan yaşamının ayrılmaz bir parçası haline gelmiştir. Geçmişi 20. yüzyılın ortalarına kadar gidiyor olmakla birlikte özellikle son yıllarda hızlanan Yapay Zekâ çalışmalarıyla birlikte fiziksel yaşam ile bilgisayar teknolojileri ve sanal fenomenler birbirinden ayrılamaz hatta bazen ayırt edilemez hale gelmiştir. Bütün bu teknolojik gelişmeler insan hayatı açısından birçok fayda getirse ve kolaylıklar sağlasa da madalyonun bir de diğer yüzü vardır. Hayatı kolaylaştırmak için insanların ve kurumların özel alanlarına giren bilgisayar teknolojileri, bir yandan da bu alanları saldırıya ve istismara açık hale getirmektedir. Kötü amaçlı kişi ve grupların eline geçen teknolojiler, kurumların altyapılarına yönelik tehdit oluşturabilmekte, gerçek kişiler bazında ise kişisel verilerin ele geçirilmesiyle insanların fiziksel, ekonomik ve siyasal güvenlikleri tehdit altına girebilmektedir.

Kişisel ve kurumsal bilgilerin yetkisiz ve kötü niyetli kişilerin eline geçmesi ve söz konusu bilgilerin kötü amaçlarla kullanılabileceği riski, "siber güvenlik" kavramının ortaya çıkmasına neden olmuştur. Siber güvenlik, siber saldırıları önlemeye veya etkilerini azaltmaya yönelik tüm teknolojileri, uygulamaları ve politikaları ifade eder. Siber güvenlik, bilgisayar sistemlerini, uygulamaları, cihazları, verileri, finansal varlıkları ve insanları kötü amaçlı yazılımlara, kimlik avı dolandırıcılıklarına, veri hırsızlığına ve diğer siber tehditlere karşı korumayı amaçlar[1].

[1] https://www.ibm.com/think/topics/cybersecurity#What+is+cybersecurity%3F (18 Ocak 2025 tarihinde erişildi)

Siber güvenliğin kişiler ve kurumlar için hayati bir ihtiyaç olduğu açıktır. Başta vatandaşların ekonomik, hukuki, sağlıkla ilgili olmak üzere her türlü alandaki verilerin, siber uzayda tutulan bilgilerin güvenliğinin sağlanması devletlerin temel sorumluluk alanlarından biridir. Fakat devletler bu görevlerini yerine getirirken sadece güvenlik penceresinden bakmamalı; bireysel hak ve özgürlüklerin kısıtlanması riskini gözetmelidir. Güvenlik riski gerekçe yapılarak insan haklarına yönelik aleyhte girişimlere başvurulmamalıdır.

Günümüzde devletler, güvenlik-özgürlük ikilemi ya da dengesi olarak adlandırılan topluma yönelik yaklaşımda ibreyi daha çok güvenlik alanına çevirmekte, bu alanı güçlendirmek adına özgürlükler alanını daraltmaktadır.

Çağımızın toplumsal yaşamının vazgeçilmez bir bileşeni haline gelen bilgisayar teknolojileri sadece kötü amaçlı kişilerin eline geçtiğinde değil, devletlerin elinde de bir otorite ve baskı aracı haline gelebilmektedir. Dinleme, izleme, takip etme ve benzeri teknolojiler, kişilerin hayatının en mahrem alanlarını ve zamanlarını bile izlemeye açık hale getirmekte, devletlerin kontrol aygıtlarının çeşitlenmesine ve güçlenmesine neden olmaktadır. Günümüzde modern devletler, Britanyalı edebiyatçı George Orwell'ın klasik haline gelmiş olan1984 romanında yarı-kurgusal bir devlet ve toplum üzerinden anlattığı ya da Fransalı düşünür Michel Foucault'un, "Gözetim Toplumu" kavramıyla açıklamaya çalıştığı gibi bütün yurttaşları farklı mekanizmalarla izlemekte ve bu izleme faaliyetini siyasal ve toplumsal bir kontrol aracı haline getirmektedir.

Bu kanun teklifinde de siber güvenliğin sağlanması bahanesiyle hak ve özgürlükler alanı daraltılmakta, siyasi iktidarı elinde bulunduranların toplum üzerindeki denetim ve kontrol mekanizmaları orantısız ölçüde genişletilmektedir. Cumhurbaşkanlığı kararnamesiyle kurulmuş olan Siber Güvenlik Başkanlığına olağanüstü yetkiler verilmektedir. Kanun teklifinde, ulusal mevzuatta daha önce bulunmayan "kritik altyapı", "kritik kamu hizmeti" gibi soyut kavramlar bulunmaktadır. Teklifte bu kavramların içeriği açık bir şekilde belirtilmemiş, bu içeriğin oluşturulması doğrudan Başkanlığa bırakılmıştır. Bu durum, yasama yetkisinin idareye devri anlamına gelmektedir[2]. Siber Güvenlik Başkanlığı hiçbir yasal düzenlemeye bağlı olmadan istediği kurumun hizmetlerini "kritik altyapı hizmeti" kapsamına alarak bu kurumun faaliyetlerini denetleme yetkisine sahip olacaktır. Hukuki öngörülebilirlik ilkesini ihlal eden bu düzenleme, aynı zamanda devletin belirli kurumları "kritik" ilan ederek, bağımsız medya

[2] "Siber Güvenlik Kanunu Teklifi Tehlikenin Farkında Mısınız?" (2025). İfade Özgürlüğü Derneği Basın Açıklaması. https://ifade.org.tr/siber-guvenlik-kanunu-teklifi-tehlikenin-farkinda-misiniz/ (18 Ocak 2025 tarihinde erişildi.)

2

kuruluşları, üniversiteler ve sivil toplum örgütleri gibi yapıları denetim altına almasına olanak tanıyacaktır.

Aşağıda maddelerin ayrıntılı değerlendirmesiyle geniş şekilde ele alacağımız bu kanun teklifi, güvenlik-özgürlük dengesinde ağırlık merkezini orantısız biçimde güvenlik tarafına kaydırmakta, vatandaşların en temel haklarının bile idari kararlarla ortadan kaldırılmasına olanak tanımaktadır.

TÜRKİYE'DE SİBER GÜVENLİK POLİTİKALARININ EVRİMİ ve YASAL ÇERÇEVE

Türkiye'de siber güvenlik politikalarının gelişimi, bilişim teknolojilerinin yaygınlaşması ve dijitalleşmenin hız kazanmasıyla doğrudan ilişkilidir. İlk dönemlerde siber tehditler daha çok bireysel güvenlik riskleri ve siber suçlarla sınırlı görülürken, zamanla bu alandaki düzenlemeler devletin kontrolünü artırmaya yönelik bir çerçeveye evrilmiştir. Türkiye'de siber güvenlik, hem kamu güvenliği hem de kritik altyapıların korunması açısından önemli bir konu haline gelirken, bu politikaların yasal dayanakları büyük ölçüde güvenlik eksenli oluşturulmuş, bireysel hak ve özgürlükler çoğu zaman ikinci plana atılmıştır. Türkiye'de siber güvenlik alanında yapılan ilk yasal düzenleme, 2007 yılında yürürlüğe giren 5651 sayılı Kanun olmuştur. Bu yasa, internet ortamında işlenen suçlarla mücadeleyi amaçlasa da aynı zamanda içerik kontrolü ve erişim engellemeleri açısından tartışmalı düzenlemeler içermektedir. Zaman içinde yapılan değişikliklerle birlikte, devletin internet üzerindeki denetim yetkisi genişletilmiş ve sansür uygulamalarına zemin hazırlanmıştır. Ancak, 5651 sayılı Kanun doğrudan siber güvenlik alanına yönelik değil, daha çok internet denetimi ve içeriğin kontrol edilmesi üzerine kurgulanmıştır. Siber güvenlik politikalarının kurumsallaşması adına 2012 yılında Ulusal Siber Güvenlik Stratejisi kabul edilmiş, 2013 yılında ise Ulusal Siber Güvenlik Kurulu oluşturulmuştur. Bu kurulun amacı, devlet kurumları ile özel sektör arasındaki koordinasyonu sağlamak ve siber tehditlere karşı ortak önlemler geliştirmektir. Ancak, uygulamada bu stratejilerin büyük ölçüde devletin güvenlik politikalarını merkezileştiren bir çerçevede kaldığı ve bireysel hakları gözeten mekanizmalar oluşturulmadığı görülmüştür.

2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu (KVKK), Türkiye'de siber güvenlik politikalarının bireysel veri güvenliği ile ilişkilendirilmesi açısından önemli bir adımdır. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü'nden (GDPR) esinlenilerek hazırlanan bu yasa, kişisel verilerin işlenmesine dair bazı standartlar getirmiştir. Ancak, uygulamada

denetim mekanizmalarının zayıflığı, KVKK'nın bireyler açısından yeterli bir koruma sağlayamamasına yol açmıştır. Devlet kurumlarının geniş yetkileri, veri sahiplerinin rızası olmaksızın kişisel verilere erişim sağlanabilmesi ve özel sektöre yönelik cezaların belirsizliği, bu yasanın etkili bir siber güvenlik politikası oluşturmasına engel olmuştur. Türkiye'deki siber güvenlik politikaları, uzun süre yürütme organının aldığı kararlar ve idari düzenlemelerle şekillenmiştir. 2018 yılında yayımlanan Cumhurbaşkanlığı Kararnamesi ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde Siber Güvenlik Daire Başkanlığı kurulmuş, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ise siber tehditleri izlemek ve müdahale etmekle görevlendirilmiştir. Ancak bu yapılar, bağımsız bir denetim mekanizmasından yoksun olduğu için yürütme erkinin kontrolü altında faaliyet göstermektedir. Günümüzde Türkiye'nin siber güvenlik politikalarına ilişkin en kapsamlı düzenleme TBMM gündemindeki Siber Güvenlik Kanunu Teklifidir. Bu teklif, siber güvenlik alanında merkezi bir otorite oluşturmayı ve Siber Güvenlik Başkanlığı adı altında yeni bir idari yapı kurmayı hedeflemektedir. Ancak, teklifin içeriği incelendiğinde, yürütme erkine geniş yetkiler tanıdığı ve temel haklar açısından ciddi riskler barındırdığı görülmektedir.

Teklifte en büyük sakıncalardan biri de kişisel verilerin korunmasına ilişkin herhangi bir yargısal denetim mekanizmasının öngörülmemesidir. Başkanlığa tanınan geniş yetkilerle, bireylerin dijital verilerine herhangi bir mahkeme kararı olmaksızın erişim sağlanabilecek ve bu süreçte bağımsız denetim mekanizmaları işletilmeyecektir. Anayasa Mahkemesi'nin daha önce 5651 sayılı Kanun kapsamında benzer düzenlemeleri iptal ettiği düşünüldüğünde, bu teklifin hukuka uygunluğu konusunda ciddi soru işaretleri bulunmaktadır. Türkiye'de siber güvenlik politikalarının evriminde dikkat çeken bir diğer nokta ise, bu politikaların çoğunlukla ulusal güvenlik perspektifinden ele alınması ve bireysel haklara yönelik güvence mekanizmalarının göz ardı edilmesidir. Avrupa ve ABD'de siber güvenlik politikaları genellikle veri güvenliği, bireysel mahremiyet ve demokratik denetim çerçevesinde geliştirilirken, Türkiye'de bu politikalar büyük ölçüde yürütme organlarının denetimsiz yetkilerini artırmak için bir araç olarak kullanılmaktadır. Siber güvenlik, elbette her devletin düzenleme yapması gereken alanlardan biridir. Ancak, bu politikalar bireylerin temel haklarını ihlal etmemeli, ifade özgürlüğünü ve özel hayatın gizliliğini zedelememelidir. Türkiye'de yürürlüğe giren düzenlemeler ve yeni yasa teklifleri değerlendirildiğinde, bireylerin mahremiyet hakkını korumaktan çok, devletin gözetim yetkisini artırmayı hedeflediği görülmektedir.

Yasa teklifinde Siber Güvenlik Başkanlığı'na tanınan geniş yetkiler, yürütme erkini yargı denetiminin üstüne çıkaran bir düzenleme olarak dikkat çekmektedir. Başkanlık, özel

şirketlerden, kamu kurumlarından ve bireylerden veri toplama yetkisine sahip olacak ve bu süreç herhangi bir hukuki denetim mekanizmasına tabi olmayacaktır. Özellikle basın kuruluşları ve dijital medya organları için bu düzenleme, gazetecilik faaliyetlerini doğrudan tehdit edebilecek niteliktedir. Türkiye'de siber güvenlik politikalarının geleceği bireysel haklar ve devletin güvenlik kaygıları arasındaki dengeyi koruyacak şekilde yeniden ele alınmalıdır. Güvenlik politikaları, otoriter bir yönetimin aracı haline gelmemeli, yurttaşların dijital haklarını koruyacak mekanizmalar içermelidir. Siber güvenlik alanında daha şeffaf, hesap verebilir ve bağımsız denetim mekanizmalarıyla desteklenen bir çerçeve oluşturulmadığı sürece, devletin bu alandaki her yeni düzenlemesi, bireysel özgürlükler açısından bir tehdit olmaya devam edecektir. Türkiye'de siber güvenlik politikalarının evrimi, bireysel özgürlüklerin korunmasını esas alan demokratik mekanizmalarla desteklenmediği sürece, uluslararası normlara uyum sağlamayacak ve hukuki meşruiyet açısından ciddi tartışmalara neden olacaktır. Yeni yasa tekliflerinin bu çerçevede gözden geçirilmesi ve güvenlik adına bireysel hakların feda edilmediği bir düzen oluşturulması zorunludur.

BU TEKLİFE NEDEN İHTİYAÇ DUYULDU?

Hayatın her evresinde oldukça yoğun bir şekilde kullanılmaya başlanan dijital olanaklar insan hayatına getirdiği kolaylıklarla beraber oldukça yoğun güvenlik problemleri de yaratmıştır. Türkiye, dijital dünyaya uyum sağlamak konusunda bazı adımlar atmış ve yurttaşların yaşamını kolaylaştıran "e-devlet", "e-nabız" gibi veri tabanlarını kullanmaya başlamıştır. Teknolojik altyapısı yeterli olmadan hızlı şekilde dijitalleşen bir ülkenin verisini koruması ve de her türlü siber saldırıya karşı hazır olması mümkün değildir. Kaldı ki Türkiye tüm bu önemli dijital hizmetlerin yazılımlarını oluşturacak nitelikli ekip ve ekipmanlara da sahip değildir. Bu durumda tüm devlet yapılarının ve yurttaşların verilerini korumak zorlaşmıştır.

Bilginin kullanılması, erişilmesi, saklanması ve paylaşılması siber ortamın yaygınlaşmasıyla beraber oldukça kolaylaşmıştır. Fakat her dönemde değerli olan bilginin günümüzde elektronik hale gelmesi ve bilişim sistemleri ile yoğun bir şekilde paylaşılması, maruz kaldığı riskleri artırmakta ve bilgi güvenliği kavramını yeniden dijital ortamlar için tartışmaya açmaktadır. Bilgiye ulaşımda zaman ve mekân açısından kolaylık sağlayan bu yöntemler beraberinde güvenlik zafiyetleri de yaratmıştır.

Türkiye'yi yönetenler kabul etmese de defalarca siber saldırılar olmuş ve yurttaşlar mağdur edilmiştir. Bu yüzden de uzunca zamandır bu konuda yasal yaptırımlara ihtiyaç vardı. Ancak

mevcut kanun teklifinde iktidarın esas amacı konusunda kafaları karıştıran maddeler mevcuttur. Verileri korumak ya da siber saldırılara karşı caydırıcı cezalardan ziyade, siber saldırı veya veri çalınması durumunda konuyla ilgili kamuoyuna bilgi vermenin suç sayılacağı kanunlar hazırlanmıştır. Bu yolla kurulacak başkanlığa verilen sınırsız yetkiler ve yasaların kötü yöneticilerin elinde keyfi uygulamalara imkân tanıması da oldukça kaygı vericidir. Dolayısıyla esasında kamu yararı için elzem olan bu kanun teklifinin hazırlanmasında iktidarın neyi murat ettiği bizim açımızdan soru işaretleri barındırmaktadır.

PANDEMİ DÖNEMİNDE YAŞANAN VERİ SIZINTILARI

2019'un Aralık ayında başlayan COVID-19 Pandemisi dönemi, dünya genelinde dijitalleşmenin hızlandığı, insanların daha fazla çevrimiçi platformları kullandığı bir süreç olmuştur. Bu durum, veri güvenliği ve kişisel verilerin korunması konusunda birtakım risklerin artmasına da neden olmuştur. Pandemi nedeniyle hem kamu hem de özel sektörde birçok insanın uzaktan çalışmaya başlanması, sağlık hizmetlerine olan yoğun talep ve dijital platformların daha fazla kullanılmaya başlanması, siber saldırılar için daha olanaklı bir ortam yaratmıştır. Türkiye'de de sağlık sektörü başta olmak üzere birçok alanda siber saldırılar artmış; sağlık hizmetlerine dair kişisel bilgiler, aşı ve test sonuçları gibi veriler siber saldırganlar tarafından hedef alınmıştır. COVID-19 pandemi döneminde 85 milyon kişinin, yani bütün vatandaşların verilerinin çalındığı iddiası, dönemin Ulaştırma ve Altyapı Bakanı Abdulkadir Uraloğlu tarafından da doğrulanmıştır.

Pandemi döneminde iş devamlılığının sağlanması, ekonomik sistemin çalışması, arz ve talep dengesinin korunması için öncelikli koşul olan uzaktan çalışma yöntemi siber saldırılara adeta bir davetiye özelliği taşımıştır. Bilişim altyapısı ve bilgi güvenliği bakımından uzaktan çalışma altyapısına sahip olamayan birçok kurum, hızlı bir şekilde uzaktan çalışma sistemine geçmiş; böylelikle siber güvenlik alanındaki zorluklar bir kez daha ortaya çıkarmıştır. Sanal alanda özel ağları bulunmayan kurum çalışanları tarafından güvenli olmayan yöntemler ile kritik verilerin kullanılması, mevcut tehditlerin azaltılması yaklaşımlarına karşı tutarsız bir yaklaşım ortaya çıkarmıştır. Ortaya çıkan siber olaylar, kurumların siber güvenliğini sağlaması, iletişim ve bilgi teknolojisi alanlarında uzaktan çalışma sistemlerini güvenilir bir duruma getirebilmeleri için daha fazla çaba göstermelerine neden olmuştur. Bu durum da kurumların teknolojinin yönetimi konusundaki zafiyetlerini ortaya çıkmıştır. Uzaktan çalışma şartları nedeniyle güvenlik

farkındalığı azalan ve kurumsal güvenlik adımlarını benimsememiş kurum çalışanları üzerinde sosyal mühendislik yönelimlerinin etkisi de artmıştır.

Sağlık Bakanlığı e-nabız sisteminden tüm yurttaşların özel nitelikli verileri olan sağlık verileri ile birlikte çok sayıda verisinin çalındığı, bu verilerin telegram hesaplarında, değişik internet sitelerinde satışa sunulduğu herkesçe bilinmektedir. Keza aynı şekilde, İç İşlerini Bakanlığının MERNİS sisteminden veri ihlallerinin yaşandığı ve hala önlem alınmadığı da bilinmektedir. MERNİS ve e-nabız sisteminde büyük açıklar olduğu halde, Sağlık Bakanlığı ve İç İşleri Bakanlığı bugüne kadar önleyici hiçbir adım atmamışlardır.

KRİZ ANLARINDA İNTERNET ERİŞİMİNİN KISITLANMASI/

SANSÜR-OTOSANSÜR

AKP iktidarı boyunca internet yasakları iletişime en çok ihtiyaç duyulan birçok kriz anında ve önemli gündemlerde uygulanmıştır; basın ve yayına getirilen sansürün etkisiyle alternatif haber alma kanallarına dönüşen sosyal medya mecraları da bu yasaklardan en büyük payı almıştır. Yasaklar silsilesi ve basında uygulanan sansür AKP iktidarının alametifarikası durumuna gelmiş, ülkede yaşananlar istibdat dönemini dahi aşmıştır. Türkiye, uzunca bir süredir basın-yayın özgürlüğünün ihlali, tutuklu gazeteciler, kapatılan yayın organları ve sosyal medyaya dönemsel olarak getirilen kısıtlamalar nedeniyle dünya gündeminde yer alan bir konumdadır. Türkiye, basın-yayın özgürlüğüne iktidarların uyguladıkları sansür mekanizmalarından kaynaklı her daim otosansür mekanizmalarının da işletildiği bir ülke olmuştur.

Krizleri çözmekte ne yarar sağladığını henüz tam olarak anlayamadığımız bu politikalar AKP iktidarı tarafından da savunulacak bir noktada değildir artık. Depremde enkaz altında kalan birçok yurttaşımız telefonla ve internetle iletişim sağlansa belki hayatta olabilecekken iktidarın çöken iletişim alt yapısı yetmezmiş gibi internete erişimi de kısıtlamasından kaynaklı can kayıpları artmıştır. Ulaştırma Bakanı Adil Karaismailoğlu, depremin hemen ardından internet iletişimini kesmeyi "Gerekiyordu demek ki" diye savunmaya çalışmıştır. Depremden günler sonra, enkazın altında cansız bedeninin yanında bulunan cep telefonundan yardım almaya çalışan küçük kız çocuğunun, bakan iletişimi kestiği için babasına ulaşamadığını öğrendik.

Deprem ve/veya silahlı saldırılar sırasında tüm sosyal medya platformlarına yönelik bant daraltma uygulaması basının haber yapma, vatandaşın da haber ve bilgi alma hakkını elinden almaktadır, tabiri caizse şalter indirilmektedir. İnternete erişimi engellemenin ve sansürün etkili

olup olmadığına veya asıl sorunun çözülüp çözülmediğine bakılmamaktadır. İki genç kadının canice bir şekilde öldürülmesiyle ortaya çıkan Discord uygulamasındaki İncel gruplarla ilgili kamuoyuna sunulmuş herhangi bir çözüm yansımadığı gibi, bu tarz uygulamalara dair sorunların devam edip etmediği veya bahse konu grupların iletişime devam edip etmediği de bilinmemektedir. Incel grupları veya başka oluşumların VPN kullanıp kullanmadıkları, VPN kullanmıyorlarsa bile başka platformlar üzerinden iletişime devam edip etmedikleri değerlendirilmemektedir.

Özcesi bu politikaların merkezinde problemi çözmek değil, gizlemek temelli bir yaklaşım vardır. Yeni kanun teklifiyle sorunlar çözülmeyip, internet erişim engeliyle sümen altı edildiğinde, bu durumun haberinin yapılması ya da söz kurulması da suç teşkil edecek hale gelmiştir.

SANSÜR YASASI İLE NE HEDEFLENMİŞTİ?

Türkiye'de iktidarın medyaya yaklaşımı her dönem özgürlükleri kısıtlamak üzerine olmuştur. Geleneksel medyanın yapısı da yandaş sermaye lehine değiştirilmiş ve ardından muhalif medyaya el koymalar ve kapatmalarla basının özgürlük alanı ortadan kaldırılmaya çalışılmıştır.

İktidarın "dezenformasyonla mücadele düzenlemesi" adı altında getirdiği "sansür yasası" 13 Ekim 2022'de yasalaşmıştı. Bugün bu yasaya dayanak gösterilerek gazeteciler, medya mensupları yargılanabilmektedir.

Kamu yararı, haberleşme özgürlüğü, sansürsüz medya ve ifade özgürlüğü gibi temel hakları içerir. Toplumun bilgilendirilmesi, farklı görüşlerin ifadesi ve demokratik katılım için bu haklar kritiktir. Ancak sansür yasaları, belirli içerikleri sınırlayarak veya sansürleyerek bu haklara müdahale edebilir. Sansür yasası ile TCK'de yeni bir suç tipi, sosyal medya kuruluşlarıyla internet haberciliği yapan sitelere yeni müeyyideler, engellemeler ve gerek kullanıcı ve gerekse sosyal medya ağ sağlayıcılarına kısıtlamalar gelmiştir. Sansür- dezenformasyon algısıyla, objektif olmayan kavramlarla, düşünce özgürlüğü ortadan kaldırılmak istenmiş; gazeteciliğin temel işlevine müdahale edilmiştir. Bu durum demokratik bir toplumun oluşması için eleştiri, haber alma ve yayma hakkına yöneltilen bir saldırıdır. Bu yasa iktidarın tüm alanlarda toplumu dizayn etme ve gerçekleri manipüle etme amacıyla ilgilidir.

Sansür Yasası ile sorgulamayan, gerçekleri ortaya çıkarmayan ve susturulmuş bir toplum hedeflenmek; muhalif ve Kürt basınının üzerinde artan baskı ve sansür yasal bir zemine

kavuşturulmak istenmiştir. Ancak kamuoyunun tepkisine rağmen yasalaşan Sansür Yasası, iktidarın hedeflediği sonuçları almasını sağlamamıştır. Yasada öngörülen cezaların mahkumiyete yeter derecede yüksek olmaması, bu yasanın tüm sosyal medya kullanıcılarını veya her türlü muhalif söylemi kapsamıyor olması iktidarı daha ağır cezalar ve suçlar düzenlemeye itmiştir.

ETKİ AJANLIĞI NEYİ AMAÇLIYORDU?

Türk Ceza Kanunu'nda ve hukuk sisteminde yer almayan yeni bir suç tipi ihdas edilerek Sansür Yasasının kapsamına alamadığı söz ve eylemler "etki ajanlığı" düzenlemesinin kapsamına alınmaya çalışılmıştır. Düzenlemeye göre herkes etki ajanı olabilir, her muhalif ve eleştirel söylem etki ajanlığı faaliyeti sayılabilir olmuştur. Bu durum modern hukukun hakim olduğu hiçbir ülke ve hukuk sisteminde yer alamayacağı gibi, demokratik ülkelerde var olması imkansız bir suç düzenlemesidir.

Başta partimiz DEM Parti olmak üzere muhalefetin yoğun baskıları sonucu son anda paketten çıkarılan etki ajanlığı düzenlemesinin özü itibariyle tamamen ajanlık suçu kapsamına girmeyen, mevcut rejim ve iktidarın çıkarlarına ve politikalarına aykırı hareket eden muhalifleri cezalandırmaya yönelik yasal çalışmalar olduğu net bir şekilde görülmektedir. Tekliften çıkarılan düzenlemede "stratejik çıkar", "talimat", "organizasyon" ve "devletin iç veya dış siyasi yararları" gibi kavramlardan da anlaşılacağı gibi son derece geniş ve muğlak olduğu gibi iktidarın keyfi ve kötü kullanıma da açık bir düzenleme söz konusuydu.

Metindeki muğlak ifadeler ve kapsadığı alanın net olmaması sebebiyle yasalaşması halinde, gazetecilerin, sivil toplum örgütlerinin, araştırmacıların kolaylıkla "etki ajanı" ilan edilip tutuklanabileceği bir yasa olarak tasarlanmıştı iktidar tarafından.

Çıkarılan sansür yasası, gazetecilerin, yurttaşların cezalandırılması yetmiyormuş gibi özgür basın mensuplarına etki ajanı damgası vurulup eleştirel akıl, muhalif sesler, özgür basın susturulmaya çalışılmıştır.

SANSÜRÜN SERENCAMI- SİBER GÜVENLİK KANUN TEKLİFİ

Sansür Yasasının beklenen etkiyi göstermemesi, Etki Ajanlığı düzenlemesinin yasadan çıkarılması üzerine iktidar veri sızıntısını önleme bahanesiyle sansürlerini içine serpiştirebileceği yeni bir düzenlemeyle karşımızda; Siber Güvenlik Yasası!

İktidar bugün Türkiye tarihinde eşi benzeri görülmemiş bir baskı rejimini medya üzerinde kurumsallaştırmaya çalışmaktadır. Hukuksuz gözaltı, tutuklamalar, tehditler, gözdağlarının yanı sıra bugün gazeteciler sansürü merkezileştirmeye çalışan bu ve benzeri yasal düzenlemelerin gölgesi altında mesleklerini ifa etmeye çalışmaktadır. Medyanın büyük bölümünü kontrolü altına almasına karşın halkın haber alma hakkının gereğini yerine getirme görevini tüm baskılara karşın sürdüren sınırlı sayıdaki yayın organı ve gazeteciyi susturamayan iktidarın son hamlesi de Siber Güvenlik Yasasıdır.

Teklifte kullanılan kavramların tıpkı Sansür Yasası ve Etki Ajanlığı düzenlemelerindeki gibi yasal açıdan belirsiz ve yoruma açık olmasının çok ciddi hak ihlallerine yol açacağı aşikardır. Bu ifadelerin çerçevesi çizilmeden ve tanımı yapılmadan kullanılmasının, yasayı uygulayacak yargı organlarının bu tanımları keyfi biçimde yorumlamasına ve hukukun sınırlarını esnetmesine imkân tanıyabileceği ortadadır.

Keyfi uygulamalara olanak tanımaları, ifade özgürlüğüne ket vurma ve iktidara karşı olan herkes için bir susturma argümanına dönüşme ihtimali üç durum için de ortak riskler barındırmaktadır. Siber Güvenliğin günümüzde elzem bir ihtiyaç olduğu noktasında hemfikir olunsa dahi, iktidarın hem sansür yasası hem etki ajanlığı hem de şu ana kadar kriz anlarında izlediği politikalara baktığımızda amacın kamu yararı olmadığı, kendilerine alan açma ve muhalif tüm sesleri susturma olduğunu rahatlıkla söyleyebiliriz.

SİBER GÜVENLİK KANUNU TEKLİFİ NELER GETİRİYOR?

Siber Güvenlik Kanunu Teklifi, Türkiye'de dijital güvenliğin sağlanması amacıyla gündeme getirilen en kapsamlı düzenlemelerden biri olarak sunulsa da içerdiği hükümler itibarıyla ifade özgürlüğü, kişisel verilerin korunması ve yürütme erkine verilen olağanüstü yetkiler açısından ciddi riskler taşımaktadır. Kanun teklifi, siber tehditlerle mücadele etmek ve kritik altyapıları korumak adına merkezi bir yapı oluşturmayı amaçlamaktadır. Ancak, teklifin ayrıntılı incelenmesi, demokratik hukuk devleti ilkeleriyle bağdaşmayan birçok yönü olduğunu ortaya koymaktadır. Özellikle ifade ve basın özgürlüğüne getirdiği kısıtlamalar, bireylerin mahremiyet haklarını ihlal eden düzenlemeler, bağımsız denetime kapalı bir yönetim yapısının kurulması

ve ağır cezai yaptırımlar teklifi sakıncalı hale getirmektedir. Günümüz dünyasında siber güvenlik, yalnızca devletlerin ve kurumların korunmasını değil, aynı zamanda bireylerin dijital haklarının da güvence altına alınmasını gerektiren bir alan olarak ele alınmalıdır. Ancak, bu teklif, bireysel hakları ikinci plana iterek, devletin dijital denetim yetkilerini genişletmeye odaklanmıştır.

Teklifin en büyük tartışma konularından biri ifade ve basın özgürlüğüne yönelik getirdiği sınırlamalardır. 16. maddede yer alan, "Veri sızıntısı olmadığı halde bu yönde algı oluşturmak" suçunun ihdas edilmesi, basın mensuplarının ve araştırmacı gazetecilerin kamu yararı açısından yaptığı haberleri potansiyel bir suç haline getirmektedir. Türkiye'de daha önce yürürlüğe giren Dezenformasyon Yasası'nın yarattığı ifade özgürlüğü ihlalleri düşünüldüğünde, bu düzenlemenin de benzer şekilde kullanılması kuvvetle muhtemeldir. Gazetecilerin devletin resmî açıklamalarından farklı veri sızıntılarına dair haber yapmaları veya bunları kamuoyuna duyurmaları suç kapsamına alınabilir. Bu durum, yalnızca basın özgürlüğüne değil, aynı zamanda halkın haber alma hakkına da doğrudan bir müdahale niteliği taşımaktadır. Avrupa İnsan Hakları Sözleşmesi'nin 10. maddesi ve Anayasa'nın 26. maddesi ile güvence altına alınan ifade özgürlüğü, bu düzenleme ile ciddi şekilde tehdit altına girmektedir. Bunun yanı sıra, teklifin içerdiği geniş yetkiler, yalnızca basın mensuplarını değil, dijital aktivistleri, sivil toplum kuruluşlarını ve hatta sosyal medya kullanıcılarını da hedef alabilecek niteliktedir. İnternet ortamında yayılan bilgilerin devletin güvenlik politikalarına uygun olup olmadığına karar verme yetkisi, yürütme erkine bırakılmaktadır. Bu tür bir düzenleme, demokratik toplumlarda olması gereken çok sesliliği ve eleştirel düşünceyi baskı altına alarak, kamuoyunda otosansürü yaygınlaştıracaktır. Özellikle hükümeti eleştiren haberlerin veya bilgi paylaşımlarının siber tehdit ya da dezenformasyon kapsamında değerlendirilerek cezalandırılması, ifade özgürlüğünün tamamen kontrol altına alınması anlamına gelmektedir.

Özel hayatın gizliliği ve kişisel verilerin korunması açısından da teklif ciddi tehlikeler barındırmaktadır. 6. madde, Siber Güvenlik Başkanlığı'na her türlü dijital veriye sınırsız erişim yetkisi tanımaktadır. Bu yetki, hakim onayı olmaksızın uygulanabilecek ve herhangi bir hukuki denetime tabi tutulmayacaktır. Normal şartlarda devletin bireylerin özel hayatına müdahale edebilmesi için güçlü bir yargısal denetim mekanizmasına tabi olması gerekirken, bu teklif bireylerin dijital mahremiyetini tamamen idarenin takdirine bırakmaktadır. Kişisel verilerin korunmasına ilişkin 6698 sayılı Kanun yürürlükte olsa da bu teklif kapsamındaki düzenlemeler, söz konusu koruma mekanizmalarını işlevsiz hale getirecek niteliktedir. Bu bağlamda, kanun teklifinde kişisel verilerin nasıl saklanacağı, hangi durumlarda kullanılacağı ve ne zaman imha

edileceği konusunda herhangi bir somut güvence yer almamaktadır. Anayasa Mahkemesi daha önce, benzer şekilde kişisel verilerin korunması hakkını ihlal eden düzenlemeleri iptal etmiştir. Ancak, bu teklifin getirdiği belirsizlikler, devletin bireylerin dijital geçmişlerini süresiz olarak saklamasına ve bu verileri keyfi şekilde kullanmasına olanak sağlayacaktır. Bu durum, yalnızca bireysel mahremiyeti değil, aynı zamanda demokratik denetimi de tehlikeye atmaktadır. Devletin veri toplama yetkisinin genişletilmesi, otoriter rejimlerin kullandığı bir gözetim mekanizmasına dönüşebilir ve yurttaşların fişlenmesine yol açabilir.

Siber Güvenlik Başkanlığı'na tanınan olağanüstü yetkiler, yürütme erkini yargısal denetimin üzerine çıkararak hukuk devleti ilkelerini zedelemektedir. Teklife göre Başkanlık, kritik altyapılar konusunda geniş yetkilere sahip olacak ve belirli kurumları siber güvenlik politikalarına uyma zorunluluğu ile karşı karşıya bırakacaktır. Ancak, kritik altyapı kavramının sınırları açık bir şekilde tanımlanmamıştır. Buna ek olarak, Başkanlık tarafından oluşturulacak Siber Olaylara Müdahale Ekipleri'nin (SOME) yetkileri de belirsizdir. SOME'lerin kimlerden oluşacağı, nasıl denetleneceği ve hangi kriterlere göre hareket edeceği konusunda net düzenlemeler bulunmamaktadır. Bu durum, yetkin olmayan, liyakat yerine siyasi sadakat esasına göre atanan bir kadronun oluşmasına neden olabilir. Yürütmeye bağlı bu yapıların bağımsız bir denetime tabi olmaması, keyfi karar alma süreçlerini ve yolsuzlukları artırabilecektir.

Siber Güvenlik Kanunu Teklifi'nin cezai yaptırımlara ilişkin düzenlemeleri de hukukun temel ilkeleri olan belirlilik, orantılılık ve ölçülülük prensipleri açısından ciddi sakıncalar içermektedir. Kanunun 16. ve 17. maddeleri kapsamında, siber güvenlik düzenlemelerine uymayan bireylere ve kurumlara yönelik ağır hapis cezaları öngörülmektedir. Ancak, bu cezaların hangi somut fiiller için uygulanacağı, suç ve cezalar arasındaki denge, keyfiliği önleyecek denetim mekanizmalarının olup olmadığı gibi kritik unsurlar açık ve net bir şekilde düzenlenmemiştir. "Veri sızıntısı olmadığı halde böyle bir algı oluşturmak" gibi son derece muğlak ve yoruma açık bir suç tanımı, keyfi yargılamalara kapı aralayarak adil yargılanma hakkını ve suçların belirli olması ilkesini ihlal etmektedir. Hukuk devletinde ceza hukuku düzenlemeleri öngörülebilir, açık ve sınırları belirli olmalıdır; ancak teklif edilen düzenleme, hukuki güvenliği yok eden geniş bir yorum alanı tanıdığı için, bireylerin ve kurumların hukuk karşısındaki konumlarını belirsiz hale getirmektedir. Cezai yaptırımların ağırlığı bakımından da teklif orantısız cezalandırma riskini beraberinde getirmektedir. Örneğin, siber güvenlik kurallarına uymayan ya da belirlenen yükümlülüklere aykırı hareket ettiği iddia edilen kişi ve kurumlara 3 yıldan 15 yıla kadar hapis cezası verilmesi öngörülmektedir. Ancak, siber

güvenliğe ilişkin düzenlemelerin ihlalinin sonuçları her durumda ağır suçlar kategorisine girecek nitelikte değildir. Cezalandırmada ağır sonuçlar doğurmayan fiiller ile ciddi zararlar doğuran eylemler arasında ayrım yapılması gerekirken, teklif bu ayrımı gözetmeksizin, siber güvenlikle ilgili herhangi bir yükümlülüğü ihlal eden herkesin ağır hapis cezasıyla karşı karşıya kalmasını mümkün kılmaktadır. Bu, yalnızca bireylerin haklarını değil, aynı zamanda özel sektörün, medya kuruluşlarının ve sivil toplum örgütlerinin faaliyetlerini de ciddi şekilde kısıtlayan bir cezalandırma rejimi yaratmaktadır. Ek olarak, yürütme erkine tanınan geniş yetkiler dikkate alındığında, bu yaptırımların belirli kişi ve gruplar üzerinde baskı kurmak amacıyla kullanılma ihtimali oldukça yüksektir. Teklifte yer alan cezai yaptırımlar keyfiliği önleyici hukuki güvencelerden yoksundur. Öngörülen suçların nasıl soruşturulacağı, delil değerlendirme süreçlerinin ne şekilde işleyeceği ve sanıkların hangi hukuki mekanizmalara başvurabileceği konusunda bir açıklık bulunmamaktadır. Ceza hukukunda suçların belirli olması gerektiği gibi, bireylerin hangi fiillerden sorumlu tutulacağı da açıkça düzenlenmelidir. Ancak, bu teklifte belirlenen cezai yaptırımlar yoruma açık ve muğlak düzenlemelere dayandığı için, yargının keyfi uygulamalarına kapı aralamaktadır. Özellikle yürütme erkinin kontrolü altındaki yargı mekanizmasının, bu muğlak suç tanımlarını genişleterek, muhalif kişi ve kurumları cezalandırma amacıyla kullanması kuvvetle muhtemeldir. Anayasa'nın 38. maddesi gereğince, suç ve cezalar ancak kanunla belirlenebilir ve bu düzenlemelerin bireylerin temel haklarını ihlal etmeyecek şekilde öngörülebilir olması gerekmektedir. Ancak, Siber Güvenlik Kanunu Teklifi, bireyleri keyfi şekilde cezalandırabilecek bir düzen kurarak, hukukun evrensel ilkelerine ve anayasaya aykırılık teşkil etmektedir. Cezai yaptırımların uygulanma biçimi ve süreci açısından adil yargılanma hakkı ve etkili başvuru mekanizmaları konusunda ciddi eksiklikler bulunmaktadır. Siber güvenlik düzenlemelerine aykırı olduğu iddia edilen fiillerin nasıl soruşturulacağı, sanıkların hangi hukuki yollarla kendilerini savunabileceği ve suçlamaların hangi delillere dayandırılacağı konusunda hukuki güvenceler sağlanmamaktadır. Kişilerin ve kurumların siber güvenlik politikalarına aykırı hareket ettiği iddiası üzerine ağır hapis cezalarıyla karşı karşıya kalması, yalnızca teknik bir hata ya da hukuki yorum farkı nedeniyle insanların yıllarca hapis yatmasına neden olabilecek bir cezalandırma mekanizmasını oluşturacaktır. Avrupa İnsan Hakları Sözleşmesi'nin 6. maddesi, adil yargılanma hakkının temel bir insan hakkı olduğunu ve cezalandırmanın hukuka uygun yargısal süreçlerle yürütülmesi gerektiğini açıkça belirtmektedir. Ancak, teklifin cezai yaptırımlara ilişkin hükümleri, bireylerin adil yargılanma haklarını ciddi şekilde zedeleyebilecek keyfi uygulamalara zemin hazırlamaktadır. Bu nedenle, kanun teklifinin cezai yaptırımlar konusunda yeniden gözden geçirilmesi, suçların tanımlarının netleştirilmesi, ceza oranlarının orantılı hale getirilmesi ve

hukuki güvencelerin açıkça düzenlenmesi gerekmektedir. Aksi takdirde, bu yasa hukukun üstünlüğü ilkesiyle bağdaşmayan ağır cezalandırma mekanizmalarıyla, temel insan haklarına ve demokratik normlara aykırı bir baskı aracı haline gelecektir.

Son olarak Siber Güvenlik Kanunu Teklifi, dijital güvenliği sağlama iddiası taşımakla birlikte, yürütme erkine geniş ve denetimsiz yetkiler tanıyan, ifade özgürlüğünü kısıtlayan, bireylerin mahremiyet haklarını ihlal eden ve cezai yaptırımları ölçüsüz bir şekilde artıran bir düzenleme niteliğindedir. Teklifin mevcut haliyle yasalaşması, demokratik hukuk devleti anlayışına zarar verecek ve Türkiye'de otoriter bir dijital denetim rejiminin oluşmasına yol açacaktır. Siber güvenlik politikaları, bireysel hakları ve özgürlükleri ihlal etmeden, şeffaf, hesap verebilir ve bağımsız denetime açık bir çerçevede şekillendirilmelidir. Bu teklifin mevcut haliyle yürürlüğe girmesi, bireylerin dijital haklarını ciddi şekilde tehdit edecek ve Türkiye'yi uluslararası normlardan daha da uzaklaştıracaktır.

ANAYASAYA AYKIRILIKLAR

Madde 7

7. Maddenin 1. Fıkrasında veri toplayan, işleyen ve benzeri faaliyetler yürüten bütün kuruluşlarının, Siber Güvenlik Başkanlığı'nın talep ettiği her türlü bilgi ve veriyi vermek zorunda olduğu belirtiliyor. Örneğin bir internet servis sağlayıcısı, Başkanlığın talebi bütün kullanıcılarının kişisel bilgilerini, konum bilgilerini, internet trafiğini vb. bilgi ve verileri vermek zorunda bırakılıyor. Bu durum, kişisel verilerin güvenliğinin ağır bir ihlali anlamına gelmektedir. Kişisel verilerin korunmasının istenmesi hakkı Anayasanın 20. Maddesinde güvence altına alınmıştır.

Daha önce 5651 sayılı *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da* bu kanun teklifinin 7. Maddesindekine benzer hükümler yer almış ancak düzenlemeler Anayasa Mahkemesi tarafından Anayasa'nın 2., 13. ve 20. maddelerine aykırı bulunarak iptal edilmiştir. İptal edilen düzenlemelere benzer düzenlemeler bu kanun teklifinde de yer almaktadır.

Anayasanın 20. Maddesinde şu ifadeler yer almaktadır: *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme*

ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Dolayısıyla, Kişisel verilerin idari bir kurum olan Siber Güvenlik Başkanlığı tarafından alınabilmesi Anayasaya aykırılık teşkil etmektedir.

8. Madde

8. maddenin 5. Fıkrasında şu ifade yer almaktadır: "Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Başkanın yazılı emri ile konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama yapılabilir ve kopya çıkarma ve el koyma işlemi gerçekleştirilebilir. Hâkim kararı olmaksızın yapılan arama ve gerçekleştirilen kopya çıkarma ve el koyma işlemleri yirmi dört saat içinde görevli hâkimin onayına sunulur." Bu maddeyle Siber Güvenlik Başkanına olağanüstü yetkiler verilmektedir. Ayrıca Ceza Muhakemesi Kanunu kapsamında olan hükümlerin (CMK 116, 119, 123, 127 md. ve devamı) başka bir kanunla değiştirilmesi, açıkça Anayasa aykırı olacaktır. Ceza Muhakemesi Kanunu temel bir kanun olup, özel kanunlarla ya da düzenlemelerle değiştirilemez. Arama ve el koyma kararının idari bir yapı olan Siber Güvenlik Başkanlığı tarafından verilmesi hukuk güvenliği ve hukuk devleti ilkesi ile bağdaşmaz. Yargı ile ilgisi olmayan bir idarecinin verdiği bir kararla yurttaşların ev ve işyerlerinin aranması, eşyalarına el konulması açıkça insan hakkı ihlali anlamına gelecektir.

Anayasa'nın 22. Maddesi haberleşme hürriyetini güvence altına almaktadır: "*Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.*" Haberleşme hakkını ve gizliliğini ihlal eden bu düzenleme Anayasaya aykırıdır.

Madde 16

Siber Güvenlik Başkanlığı Kanunu olarak komisyona getirilen bu kanun teklifinin 16. Maddesi, hukuk sistemimizde bugüne kadar var olmayan yeni suç ve cezalar ihdas etmektedir. Bilindiği üzere, devletin tekelinde bulunan cezalandırma yetkisinin kullanımına dair özgün bir alan olarak gelişmiş ceza hukuku başlı başına kritik bir disiplindir.

Kişilerin hürriyetlerini sınırlama ve hapsetme gibi ağır sonuçları olan ceza maddeleriyle ilgili yapılacak her türlü düzenleme, en başta cezanın amacı, işlevi, ölçülülüğü ve gerekliliği gibi denetimlere tabi tutulmalıdır. Bugüne kadar, Türk Ceza Kanunu'nda çok sayıda değişiklikler yapılmış, bunların bir kısmı kazuistik yöntemlerle, bir kısmı değişen sosyoloji ve siyasi tercihlere bağlı olarak yapılırken, bir kısmı ise çeşitli zamanlarda ihtiyaçlara yönelik düzenlemeler olmuştur. Buradaki en önemli nokta ise ceza hukukuna dair yapılan düzenleme ve değişikliklerin Ceza alanında uzman hukukçuların katkılarıyla yapılması ve gerçek bir toplumsal, hukuki ihtiyaca yönelik olup olmadığının doğru tespit edilmesidir. Aksi halde devletin tekelinde bulunan cezalandırma yetkisi soyut, keyfi ve ölçüsüz şekilde kullanılarak hukuk devleti olma ilkesini ortadan kaldırma riski taşıyacaktır. Tam da burada söz konusu teklifin öncelikli olarak Milli Savunma Komisyonu'na gelmesi eksik ve hatalıdır. Cezai düzenlemeler içeren bu kanunun Adalet Komisyonu tarafından incelenmesi, değerlendirilmesi gerekmektedir. Kanunu hazırlayanlar, Siber Güvenlik Başkanlığı kuruluşunu aşan şekilde maddeler ekleyerek kanuni bütünlüğü ve hukuki güvenilirliği ihlal etmiştir.

İhdas edilen suçun ve cezanın hukuk sisteminde ve toplumsal ilişkilerde yaratacağı etkiler, sonuçları, diğer temel hak ve özgürlüklerle ilişkileri oldukça titiz bir şekilde irdelenmeli, değerlendirilmelidir. Söz konusu teklifin 16. Maddesindeki düzenlemeler pek çok temel insan hakkı açısından riskler içermektedir.

16. madde içerdiği düzenlemelerle Anayasa'nın temel ilkelerine, hak ve özgürlüklere ciddi şekilde aykırılık teşkil etmektedir. Öncelikle, maddenin içerdiği yetkilendirmeler, Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği ve 22. maddesinde düzenlenen haberleşme hürriyeti ile açık bir çelişki içindedir. Denetim görevlilerine tanınan geniş yetkiler, kişisel verilerin korunması hakkını ihlal ederken, bu verilerin toplanması ve kullanılması ile ilgili somut ve ölçülebilir bir sınırlandırma getirilmemektedir. Verilerin hangi amaçla ve nasıl korunacağına dair bir güvence sağlanmaması, hukuk devleti ilkesinin temel unsurlarından biri olan hukuki öngörülebilirlik ilkesini de zedelemektedir. Bu durum, bireylerin anayasal güvence altındaki haklarına yönelik ciddi bir tehdit oluşturmaktadır.

Madde ayrıca, ifade özgürlüğü ve basın özgürlüğü bakımından da önemli sorunlar barındırmaktadır. Özellikle "veri sızıntısı olmadığı halde algı oluşturma" fiilinin suç olarak düzenlenmesi, Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü ve 28. maddesinde korunan basın özgürlüğü ile bağdaşmamaktadır. Bu tür muğlak ve soyut bir düzenleme, gazetecilik faaliyetlerini baskı altına alabilecek bir mekanizma yaratmakta ve halkın bilgi edinme hakkını ciddi şekilde tehdit etmektedir. İfade özgürlüğü üzerindeki bu sınırlama, Anayasa'nın 13. maddesinde yer alan "ölçülülük" ilkesiyle de açık bir şekilde çelişmektedir. Ayrıca, cezaların caydırıcılıktan ziyade eleştirel medya ve sosyal medya kullanıcılarını sindirme amacı taşıdığına dair güçlü bir izlenim yaratmaktadır. Yine "siber uzaydaki milli güç unsurları" gibi hukuki olarak tanımlanmamış ve sınırları belirsiz kavramlarla ağır cezalar öngörerek, Anayasa'nın 13. ve 38. maddelerinde düzenlenen suç ve cezada belirlilik ilkesine aykırılık teşkil etmektedir. Suç ve cezanın belirsiz bir zemine oturtulması hem hukuki güvenlik ilkesini zayıflatmakta hem de bireylerin hangi fiillerin suç teşkil edeceğini öngörmesini imkansız hale getirmektedir. Bu durum, adil yargılanma hakkını da ihlal ederek, demokratik toplum düzeni ve hukuk devleti ilkesi ile bağdaşmayan sonuçlara yol açmaktadır. Tüm bu nedenlerle, 16. madde Anayasa'nın 13, 20, 22, 26, 28 ve 38. maddelerine aykırıdır ve iptal edilmesi gerektiği açıktır.

Teklifin 16'ncı maddesinin 1'inci fıkrası,

"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." Şeklindedir.

Öncelikle bu fıkra, oldukça geniş yetkiler tanımakta, aynı zamanda bu yetkiler kullanılırken muhatap olunacak kişi ve kurumları cezai tehdit altında bırakmaktadır. İdari bütünlük ve hukuki tutarlılık açısından bakıldığında, bu derece geniş ve olağan üstü yetkilere sahip çok az kamu kurumu olduğu ortadadır. Yargı kurumlarının dahi belirli bir davada bir kişi ve kurumdan talep ettiği veri, bilgi, belgeleri istemesi sonucunda bu denli ağır cezalar öngörülmemişken, somutlaştırılmamış amaçlar için bu yetkiyi tanımak hukuka aykırıdır.

"Kanunla yetkilendirilen mercilerin ve görevlilerin görev ve yetkileri kapsamında istedikleri bilgi, belge, yazılım, veri ve donanım" ibaresi oldukça geniş ve belirsizdir. Herhangi bir görev gerekçe gösterilerek kişi ve özel kurumlardan özel veri niteliğindeki verilerin temin edilebilir

olması başta kişisel verilerin gizliliği, güvenliği olmak üzere Anayasal güvence altındaki özel hayatın gizliliğini koruma hakkını da ihlal etmektedir. Fıkrada, açık ve net olarak somut ve yakın tehlikeden veya amaca uygunluk ölçütlerinden bahsedilmemiştir. Yakın geçmişte meydana gelen olaylar ve üst düzey devlet görevlilerinin yaptığı itiraflardan da anlaşılacağı üzere, Türkiye, teknik ve dijital olarak sahip olmadığı imkanların aksine çok hızlı dijitalleşmiş ve bu durum 85 milyonun verilerinin kamu kurumları üzerinden ele geçirilmesiyle sonuçlanmıştır. Siber Güvenliğe dair önlemlerin alınmasında gecikmeler, ihmaller ve eksikler yaşanmış söz konusu Kanun ise bu ihmallerin telafisine değil, daha fazla gerçekleşmesine veya yaşanan veri sızıntı ve çalınma vakalarının üstünün örtülmesine yönelik önlemleri önceleyen bir akılla hazırlanmıştır.

Yine Sağlık Bakanlığı "e-nabız" sisteminden tüm yurttaşların özel nitelikli verileri olan sağlık verileri ile birlikte çok sayıda verisinin çalındığı, bu verilerin telegram hesaplarında, değişik internet sitelerinde satışa sunulduğu herkesçe bilinmektedir. Keza aynı şekilde, İç İşlerini Bakanlığının MERNİS sisteminden veri ihlallerinin yaşandığı ve hala önlem alınmadığı da bilinmektedir.

MERNİS ve e-nabız sisteminde büyük açıklar olduğu halde, Sağlık Bakanlığı ve İçişleri Bakanlığı bugüne kadar önleyici hiçbir adım atmamışlardır. Dolayısıyla veri sızıntı ve ihlalleri kamu kurum ve kuruluşları tarafından veya onlar üzerinden gerçekleştirilirken, her türlü kişisel ve özel veriye ulaşım yolunun kolaylaştırılması kabul edilebilir değildir. Siber güvenlik zafiyetinin sona erdirilmesi ve tüm önlemlerin alınması gerekirken, SGB aracılığıyla, muğlak amaçlar doğrultusunda verilerin toplanması kabul edilemez.

Tüm bunların yanı sıra, ceza hukuku temel ilkeleri bağlamında ele alındığında 16. Maddenin 1. Fıkrasının bir ceza kanunu olarak hapis cezası veya adli para cezasıyla cezalandırılması evrensel ceza hukuku ilkelerine aykırıdır. İdari bir yaptırım veya Kabahat niteliğinde olan bir eylemin cezai yaptırıma tabi kılınması Anayasaya aykırılık teşkil etmektedir.

Teklifin 16'ncı maddesinin 5'inci fıkrası,

Siber Güvenlik Kanunu Teklifi'nin 16. maddesinin 5. fıkrasında komisyon toplantısında yapılan değişiklikle, "siber uzayda veri sızıntısı olmadığı halde halk arasında endişe, korku ve panik

yaratmak ya da kurumları veya şahısları hedef almak amacıyla veri sızıntısı yapılmış gibi içerik oluşturanlara ve/veya bu içerikleri yayınlayanlara iki yıldan beş yıla kadar hapis cezası verilir" düzenlemesi getirilmiştir. Bu değişiklik, önceki taslakta yer alan "algı oluşturma" ifadesini kaldırarak, halk arasında panik yaratma saikiyle suç işlenmesi unsurunu vurgulamış gibi görünse de yapılan değişiklik özünde hukuki belirsizlikleri gidermemiş ve özgürlükleri kısıtlayan nitelikte kalmıştır. Türk Ceza Kanunu'nun 217/A maddesi ile büyük ölçüde benzerlik taşımakta ve hukuki açıdan aynı sakıncaları içermektedir. TCK 217/A gibi muğlak ve sübjektif bir suç tanımına dayanarak gazetecilik faaliyetlerini ve ifade özgürlüğünü cezalandırmaya riski taşımaktadır.

TCK 217/A maddesi "Sırf halk arasında endişe, korku veya panik yaratmak saikiyle, ülkenin iç ve dış güvenliği, kamu düzeni ve genel sağlığı ile ilgili gerçeğe aykırı bir bilgiyi, kamu barışını bozmaya elverişli şekilde alenen yayan kimse, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır." hükmünü içermektedir. Bu düzenleme, hukuki belirlilik ve öngörülebilirlik ilkeleriyle çelişmekte, ceza hukukunun temel prensiplerine aykırı bir yorum alanı oluşturmaktadır. Suçun temel unsurları arasında, "halk arasında korku ve panik yaratma saiki" gibi son derece sübjektif ve yoruma açık bir unsur bulunmaktadır. Aynı şekilde 16. maddenin 5. fıkrasında da "veri sızıntısı yapılmış gibi içerik oluşturma" fiilinin halk arasında korku ve panik yaratma saikiyle işlenmiş olması suçun oluşması için yeterli görülmektedir. Ancak, bir içeriğin toplumda korku ve panik yaratıp yaratmadığı nasıl tespit edilecektir? Bunu kim belirleyecektir? Hangi kıstaslara dayanarak böyle bir saik isnat edilecektir? Bu belirsizlik, bu düzenlemeyi Anayasa'da düzenlenen suçta ve cezada belirlilik ilkesine açıkça aykırı hale getirmektedir.

Bu düzenlemenin gazetecilik mesleği açısından doğrudan bir tehdit oluşturduğu açıktır. Basın özgürlüğü, Anayasa'nın 28. maddesi ile güvence altına alınmıştır. Gazetecilik, yalnızca devletin resmî açıklamalarını tekrar etmek değil, kamu yararını ilgilendiren olayları araştırmak, doğrulamak ve halkı bilgilendirmektir. Ancak bu madde, yetkililer tarafından reddedilen veya doğruluğu sorgulanan herhangi bir haberin "veri sızıntısı yapılmış gibi gösterme" suçlamasına tabi tutulmasına imkân tanımaktadır. Geçmişte Sağlık Bakanlığı, İçişleri Bakanlığı ve Ulaştırma Bakanlığı gibi birçok kamu kurumuna ait verilerin sızdırıldığı ve bu sızıntıların gazeteciler tarafından kamuoyuna duyurulduğu bilinmektedir. Ancak, bu yasa ile birlikte,

gazetecilerin bu tür haberleri yayımlaması doğrudan suç kapsamına alınacaktır. Örneğin, bir gazeteci devlet yetkililerinin yalanladığı bir veri sızıntısını haber yaptığında, yetkililer bu haberi "halk arasında korku ve panik yaratmaya elverişli" olarak değerlendirebilir ve ilgili gazeteci hakkında soruşturma başlatılabilir. Bu durum, basın özgürlüğüne ve halkın haber alma hakkına ağır bir darbe vuracaktır.

Düzenleme ayrıca, sosyal medya kullanıcılarını da doğrudan hedef almaktadır. Günümüzde, kamuoyunun büyük bir kısmı haberleri ve olayları sosyal medya platformlarından takip etmektedir. Ancak, bu düzenleme ile birlikte herhangi bir birey, devletin resmî açıklamalarından farklı bir iddiayı veya bilgiyi paylaştığında, halk arasında korku ve panik yaratmaya yönelik hareket ettiği gerekçesiyle cezalandırılabilir. Bu durum, otosansürün yaygınlaşmasına ve demokratik tartışma ortamının tamamen ortadan kalkmasına yol açacaktır. Örneğin, bir sosyal medya kullanıcısı, bir kamu kurumuna ait sistemlerde güvenlik açığı tespit ettiğini belirten bir paylaşım yaptığında, yetkililer bu paylaşımı halk arasında korku ve panik yaratmaya yönelik olarak değerlendirebilir ve kişiyi suçlu ilan edebilir. Bu, bireylerin ifade özgürlüğünü ağır şekilde kısıtlayan bir düzenlemedir. Bu maddenin hukuki güvenlik açısından bir diğer ciddi sorunu ise, suçun hangi eylemlerle işleneceğinin açık bir şekilde tanımlanmamış olmasıdır. TCK 217/A maddesinde olduğu gibi, burada da "veri sızıntısı yapılmış gibi içerik oluşturmak" fiilinin ne şekilde gerçekleştirileceği belirtilmemiştir. Suç tanımı "serbest hareketli" bir suç olup, hangi davranışların suç teşkil edeceği konusunda ciddi belirsizlikler içermektedir. Örneğin, bir haber sitesinin daha önce sızdırılmış ve kamuoyunda dolaşan bir belgeyi yayımlaması bu kapsamda değerlendirilecek midir? Peki, bir vatandaşın devletin bir açıklamasını eleştirerek, siber güvenlik ihlali ihtimalini gündeme getirmesi suç sayılacak mıdır? Bu tür soruların net yanıtlarının bulunmaması, bu düzenlemenin hukuki belirlilik ilkesini ihlal ettiğini göstermektedir. Bu düzenleme demokratik toplumun en temel unsurlarından biri olan kamu denetimi mekanizmasını yok etmektedir. Özgür basın, devleti ve kamu kurumlarını denetleme işlevi görerek, toplumun daha şeffaf ve hesap verebilir bir yönetime sahip olmasını sağlar. Ancak, bu tür yasalar, devletin eleştirel haberleri ve kamusal tartışmaları baskı altına almak için hukuki araçlar geliştirdiğini göstermektedir. Daha önce TBMM'ye getirilip sonra geri çekilen Etki Ajanlığı düzenlemesinin temelinde yatan baskıcı zihniyet, şimdi bu kanun teklifinin satır aralarına gizlenerek yürürlüğe sokulmaya çalışılmaktadır.

Tüm bu değerlendirmeler ışığında, 16. maddenin 5. fıkrası, Anayasa'ya açıkça aykırıdır. Hukuki öngörülebilirlikten yoksun, keyfi uygulamalara açık, basın ve ifade özgürlüğünü doğrudan hedef alan bir düzenlemenin hukuk devleti ilkeleriyle bağdaşması mümkün değildir. Bu nedenle maddenin mevcut haliyle yasalaşması, yalnızca gazetecileri ve medya kuruluşlarını değil, her bireyin ifade özgürlüğünü tehdit eden ağır bir sansür rejimi yaratacaktır.

Teklifin 16'ncı maddesinin 6'ncı fıkrası,

Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü oluşturan unsurlara yönelik saldırılara ağır cezalar öngörmektedir. Düzenleme, milli güvenliği koruma amacı taşıyor gibi görünse de "siber uzaydaki milli güç unsurları" ifadesinin hukuki olarak tanımlanmamış olması ciddi bir belirsizlik yaratmaktadır. Bu muğlaklık, hangi eylemlerin suç kapsamında değerlendirileceği konusunda geniş yorumlara ve keyfi uygulamalara zemin hazırlayabilir. Ayrıca, cezaların 8 ila 15 yıl gibi yüksek oranlarda belirlenmesi, bu tür suçların niteliğiyle orantılı olmayan bir cezalandırma anlayışı sergileyerek adil yargılanma hakkını ve hukuki güvenlik ilkesini zedeleme riski taşımaktadır. Bu tür cezaların caydırıcılığı artırmak yerine ifade ve bilgi özgürlüğünü baskı altına alabileceği de göz önünde bulundurulmalıdır. Fıkra, elde edilen verilerin siber uzayda bulundurulmasını veya yayılmasını da cezalandırmakta, bu kapsamda bilgi ve belgelerin açıklanmasının suç teşkil edebileceği belirtilmektedir. Ancak, kamu yararını ilgilendiren bilgilerin kamuoyuna açıklanması durumunda dahi ağır cezalar öngörülmesi, özellikle gazetecilerin ve ifade özgürlüğünü kullanan bireylerin üzerinde ciddi bir baskı yaratabilir. İnsan hakları bağlamında, bu tür düzenlemeler Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) ifade özgürlüğü ile ilgili 10. maddesiyle çelişecektir. Ayrıca, milli güvenliği gerekçe göstererek bu kadar geniş kapsamlı bir cezalandırma mekanizması öngörülmesi, bireylerin ve medyanın kamu denetimi yapma işlevini zayıflatabilir.

Hukuki açıdan bakıldığında, bu düzenlemenin keyfi yorum ve uygulamalara açık olduğu açıktır. "Milli güç unsurları" ifadesinin sınırlarının belirlenmemiş olması, bireylerin hangi eylemlerinin suç sayılacağının önceden öngörülebilir olmasını engellemektedir ki bu durum suç ve cezada belirlilik ilkesiyle çelişir. Ayrıca, düzenleme, kişisel haklar ile kamu yararı arasındaki dengeyi kurmakta yetersiz kalmaktadır.

SONUÇ

Türkiye dünyada en hızlı dijitalleşen ülkelerden biridir. Ancak yeterli teknolojik altyapısı olmadan bu kadar hızlı dijitalleşen bir ülkenin verisini koruması ve siber saldırılara karşı hazır olması olanaklı değildir. Teknoloji üretmeyip sadece kullanıcısı olunan bir durumda, bu kolaylığın ağır bedelleri de olabilmektedir.

Global dünyada, dijital yaşamın her yeri sarıp sarmaladığı bir dönemde verilerin sınır ötesine çıkmasını önlemek neredeyse olanaksızdır. Ancak önemli olan verilerin ne şekilde gittiği ve hangi verilerin gittiğidir. Ancak bugün Ulaştırma ve Altyapı Bakanlığı ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi gibi ilgili kurumlar bir yandan "Türkiye'nin verisi Türkiye'de" kalacak gibi büyük laflar ederken, diğer yandan da 85 milyon yurttaşın verisini depolayıp koruyacak bulut depolama sisteminin, yeterli depolama alanına sahip sunucuların olmadığı da bilinen bir gerçektir. Kaldı ki büyük veriyi elinde bulunduran Google, Microsoft, META (facebook, instagram ve whatsapp'a sahip olan şirket) gibi büyük şirketler, çocuklar da dahil olmak üzere neredeyse 85 milyon yurttaşın verilerini zaten ele geçirmiş durumdadır.

Bu kanun teklifinin, ihtiyaç duyulan teknik düzenlemeler dışında asıl amacının medya kuruluşlarına, özellikle de bağımsız medya kuruluşlarına dolaylı olarak sansür uygulamak olması, başlı başına temel ihtiyacının dışına çıkaran haksız ve hukuksuz bir düzenleme görüntü vermesine neden olacaktır.

Bu teklifte de AKP iktidarı, her zaman uyguladığı taktiği uygulamakta, yapmak istediği şeyin tam tersini iddia etmektedir. Bu kanun teklifi sunulurken "siber uzaydaki kişisel verilerin sağlanması"nın amaçlandığı iddia edilmiştir ancak bu teklif kanunlaşırsa bir idari kuruluşa (Siber Güvenlik Başkanlığı) bütün kurumların, şirketlerin, vatandaşların verilerine hiçbir kısıtlama olmaksızın erişme yetkisi verilecektir. Dolayısıyla hiçbir kişi ve kurumun verilerinin gizliliği kalmamış olacaktır.

Çünkü siyasi iktidar, bugüne kadar teknolojik olanakları büyük ölçüde kendisiyle aynı siyasi çizgide yer almayan kişi ve kuruluşların sesini kısmak için kullanmaktadır. Basın kuruluşlarına, sivil toplum kuruluşlarına ve genel olarak vatandaşlara yönelik sansür uygulamalarının sadece son dönemlerdeki birkaç örneğine bakacak olursak bu durum çok daha net bir şekilde görülecektir;

1- Millî güvenlik ve kamu düzeninin korunması gerekçesiyle engellenen ve/veya Türkiye'den erişilmesine kısıtlama getirilen bazı X (eski adıyla Twitter) hesapları:
   - Mezopotamya Ajansı: @MAturkce
   - JINNEWS Haber Ajansı: @jinnewsturkce
   - Yeni Yaşam Gazetesi: @yeniyasamgazete
   - Siyasi Haber: @SiyasiHaberOrg

2- ETHA, Gazete Patika, Kızıl Bayrak, Özgür Gelecek, Umut Gazetesi ve Yeni Demokrasi, millî güvenlik ve kamu düzeninin korunması gerekçesiyle, Ankara 10. Sulh Ceza Hakimliğinin 8 Ocak 2025 tarihli ve 2025/558 sayılı kararıyla erişime engellendi. Alınteri Gazetesi ve Devrimci Demokrasi de aynı kararla erişime engellendi.

3- Yeni Yaşam Gazetesi, millî güvenlik ve kamu düzeninin korunması gerekçesiyle, Diyarbakır 4. Sulh Ceza Hakimliğinin 2 Ocak 2025 tarihli ve 2025/7 sayılı kararıyla erişime engellendi.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanlığı, hemen hemen bütün toplumsal olaylardan sonra hiçbir yargı kararına dayanmaksızın bant daraltması uygulamasına gitmekte, Anayasal güvence altında olan haberleşme hakkını ihlal etmektedir. Örneğin, yukarıda da bahsedildiği gibi, 6 Şubat 2023 depremi sonrasında BTK tarafından sosyal medya platformlarına yönelik "bant daraltması" uygulaması yapılmış; bu uygulama, kurtarma çalışmaları için organize olmaya çalışan kurumların ve vatandaşların çabalarının aksamasına neden olmuştur.

Siber Güvenlik Kanunu Teklifi, siber uzaydaki verilerin ve kişisel bilgilerin güvenliğini sağlama iddiasında olan bir düzenleme olarak temel hak ve özgürlüklerin korunması ilkesiyle uyum içinde olmalıdır. Fakat kanun teklifinin mevcut hali temel hak ve özgürlüklerin korunması bir yana, ifade özgürlüğü, kişisel verilerin korunması ve özel hayatın gizliliği gibi demokratik toplumun temel değerlerini ciddi şekilde tehlikeye atmaktadır[3].

[3] "Siber Güvenlik Kanunu Teklifi Tehlikenin Farkında Mısınız?" (2025). İfade Özgürlüğü Derneği Basın Açıklaması. https://ifade.org.tr/siber-guvenlik-kanunu-teklifi-tehlikenin-farkinda-misiniz/ (18 Ocak 2025 tarihinde erişildi.)

Bu teklif kanunlaşırsa, ortaya olağanüstü yetkilere sahip, denetimden muaf tutulmuş bir idari kuruluş çıkacaktır. Bu kuruluşun faaliyetleri, vatandaşların en temel haklarının her an ihlal edilme riskini doğuracaktır. Bu bilgi ve değerlendirmeler çerçevesinde; Siber Güvenlik Kanunu Teklifiyle ilgili temel önerilerimiz şu şekildedir:

1. Kanun teklifi geri çekilmeli; temel hak ve özgürlükler perspektifini esas alan bir yaklaşımla ilgili tüm tarafların görüşlerine başvurularak tekrar ele alınmalı ve bu çerçevede yeniden düzenlenmelidir. Yeniden değerlendirme yapılırken küresel ölçekte başta Birleşmiş Milletler ve Avrupa Konseyi'nin ilgili metinleri olmak üzere uluslararası düzenlemeler; ulusal mevzuatta ise Anayasa ile 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda bulunan düzenlemeler dikkate alınmalıdır.
2. Siber Güvenlik Başkanlığına olağanüstü yetkiler veren ve her türlü denetimden muaf kılan bütün düzenlemeler kanun teklifinden çıkarılmalıdır. İdari bir kurum olan Başkanlık, şeffaf, hesap verebilir ve denetime açık bir kamu kurumu olarak yeniden tasarlanmalıdır.
3. Başta "kritik altyapı" ve "kritik kamu hizmetleri" gibi kavramlar olmak üzere daha önce hukuk mevzuatında bulunmayan ve içeriği muğlak kavramlar teklif metninden çıkarılmalıdır. Teklif metnindeki bütün kavramlar, kurumlar ve düzenlemeler öngörülebilir ve anlaşılabilir olmalıdır.
4. Kanun teklifinde ifade özgürlüğüne kısıtlama getirebilecek hiçbir düzenleme bulunmamalıdır. Özel olarak basın kuruluşları ve gazeteciler, genel olarak ise bütün toplum üzerinde sansür uygulamasına yol açabilecek hiçbir düzenleme kanun metninde yer almamalıdır. Kişileri ve kuruluşları otosansüre yönlendirebilecek ifadeler de kanun metninden çıkarılmalıdır.
5. Siber güvenliğin sağlanmasına yönelik düzenlemeler; uzmanlar, sivil toplum kuruluşları, meslek örgütleri, hukukçular ve diğer bütün ilgili taraflar dahil edilerek yürütülecek bir tartışma sürecinin sonunda yapılmalıdır.

Vezir Coşkun Parlak
Hakkâri

Onur Düşünmez
Hakkâri

MUHALEFET ŞERHİ

2/2860 Esas sayılı Siber Güvenlik Kanunu 10/01/2025 tarihinde Meclis Başkanlığına sunulmuştur. Teklif, 15/01/2025 tarihinde Milli Güvenlik Komisyonunda görüşülmüştür. Komisyon görüşmeleri sonucunda 2, 8 ve 16 ncı maddelerde değişiklik yapılarak teklif biri geçici olmak üzere yürütme ve yürürlük maddeleriyle birlikte toplam 21 maddeden oluşmaktadır.

USULE İLİŞKİN DEĞERLENDİRMELERİMİZ

1. Anayasaya Aykırılık Sorunu:

Anayasanın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri belirliliktir. Belirlilik ilkesi hukuki güvenlik ilkesi ile doğrudan bağlantılıdır. Hukuki Güvenlik ve Belirlilik; hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu sarsıcı düzenlemelerden kaçınmasını gerektirir. Yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması ayrıca kamu gücünün keyfi ve orantısız kullanılamayacağını ifade eder.

Bu bakımdan kanunun metni, bireylerin gerektiğinde hukuki yardım almak suretiyle hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını açıklık ve kesinlikle öngörülebilmelerini sağlayacak şekilde yazılmalıdır. Ez cümle kanun kapsamında kalacak iş ve işlemler veyahut uygulamalar için taraflar muhtemel etki ve sonuçları ön görebilmelidir. Siber Güvenlik Kanun teklifi, içinde bulunduğumuz teknoloji çağında milli güvenlik açısından son derece gerekli ve önemlidir. Ülkemizin coğrafi konumu, dünyanın içinde bulunduğu kaotik dönem de göz önünde bulundurulduğunda siber güvenliğe ilişkin bir düzenleme yapılması kaçınılmaz bir gerçektir. Gerek terörle mücadele gerekse kurumlarımızın her türlü dijital saldırıdan korunması amacıyla bu konuda yasal bir düzenlemeye ihtiyaç duyulmaktadır. Ancak kanun teklifinin içerisinde bulunan bazı maddeler nedeniyle Anayasaya aykırılıklar barındırdığını bu sebeple kanun teklifinin öncelikle Anayasa Komisyonunda ve Adalet Komisyonunda görüşülmesi gerektiğini düşünüyoruz.

Anayasanın sair maddelerinde özel hayatın gizliliği, konut dokunulmazlığı, haberleşme hürriyeti gibi temel haklar korunmaktadır. Bu hakların hangi şekilde korunacağı da yine Anayasa da tarif edilmektedir.

Anayasanın Özel Hayatın Gizliliği başlıklı 20 nci maddesinin ikinci fıkrası açıkça şöyle ifade edilmiştir; *"Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar."* maddenin açık hükmünden anlaşılacağı üzere Siber Güvenlik Kanun Teklifinin 8 inci maddesinin beşinci fıkrası açıkça Anayasaya aykırıdır. Ayrıca teklifin aynı maddesi yargı organları tarafından yerine getirilecek iş ve işlemlere yasamanın açıkça müdahalesi anlamına gelmektedir. 5271 sayılı Ceza Muhakemesi Kanunun 116 ila 134 üncü maddeleri arasında arama ve el koyma hükümleri düzenlenmiştir. Buna göre; "*Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri arama yapabilirler. Ancak, konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının yazılı emri ile yapılabilir. Kolluk amirinin yazılı emri ile yapılan arama sonuçları Cumhuriyet Başsavcılığına derhal bildirilir."*

Yasama, yürütme ve yargı erklerinin birbirinin görev alanına giren konulara yetkisi olmadan müdahale etmesine fonksiyon gaspı denilmektedir. Fonksiyon gaspı niteliğindeki işlemler idare hukuku açısından yok hükmündedir. Teklifle düzenlenmek istenilen yetki Anayasa ve kanunlarla hâkim ve savcılara verilmiştir. Mevzuatın açık hükmünden anlaşılacağı üzere siber güvenlik başkanının sanki hâkim veya savcıymış gibi bu göreve denk yetkilerle donatılması Anayasaya aykırı olup idare hukuku açısından da fonksiyon gaspıdır.

Anayasanın Konut Dokunulmazlığını düzenleyen 21 inci maddesinde "*Kimsenin konutuna dokunulamaz. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin konutuna girilemez, arama yapılamaz ve buradaki eşyaya el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.*" Anayasa yetkili kılınmış merciin yazılı emri bulunmadıkça teklif

içerisinde bulunan kapalı alanlarda arama yapmayı, kopya çıkarmayı ve el koymayı yasaklamıştır. Anayasanın bu hükmü dolanılarak yetkili kişiler arasına Siber Güvenlik Başkanının eklenilmeye çalışılması da hukuka aykırıdır.

Komisyon görüşmelerinde iktidar partisi teklifteki hukuka aykırılığa komisyon üyeleri tarafından gösterilen tepkiler üzerine bir önerge sunmuş ve önerge kabul edilmiştir. Ancak ne önerge ne de gerekçesi hukuka aykırılığı ortadan kaldırmamıştır. Önerge gerekçesinden, gecikmesinde sakınca bulunan hâllerde arama ve el koyma yetkisinin cumhuriyet savcısına da tanınacağı, bu işlemlerin "millî güvenlik, kamu düzeni, suç işlenmesinin veya siber saldırıların önlenmesi amacıyla" gerçekleştirilebilmesi ve bu işlemlerin makul sebeplerle yapıldığının gerekçelendirilmesine ilişkin düzenleme yapılmak istenmiştir ancak bu yetki zaten Anayasa ve CMK ile savcılarda vardır. Teklifle, Anayasa ve CMK'da hâkim ve savcılara verilen bu yetki siber güvenlik başkanına da tanınmak istenmektedir. Komisyon üyelerinin itirazları üzerine AK Parti üyeleri tarafından hazırlanan bu önerge kanunun muhteviyatında bir değişiklik meydana getirmemiştir.

Bu kısımda değinmek istediğimiz son husus ise 8 Ocak 2025 tarihinde yayınlanan resmî gazetede Cumhurbaşkanlığına bağlı Siber Güvenlik Başkanlığının kurulmuş olmasıdır. Teklif komisyonda 15 Ocak 2025 tarihinde görüşülmeye başlanmıştır. Bu durum bize yakın tarihte bir bakanın siz işlemi yapın karar arkadan gelir anlayışını hatırlatmaktadır. Mevcut iktidar yüce meclisin bu kanun teklifi üzerinde yapacağı çalışmaları görmezden gelerek henüz teklif yasalaşmadan ve hatta görüşmelerine dahi başlanmadan ilgili başkanlığın kurulduğunu ilan etmiştir. Bu işlemle millet iradesinin ayaklar altına alındığı bir örnek daha görülmektedir.

2. Teklifin Komisyonda görüşülme süreci hakkında:

Türkiye Büyük Millet Meclisine sunulan kanun tekliflerinin komisyonlara havale işlemleri İç Tüzüğün 23 üncü maddesine göre yapılmaktadır. İlgili madde gereğince raporu Genel Kurul görüşmelerine esas olacak komisyona esas komisyon, işin kendilerini ilgilendiren yönü veya maddeleri üzerinde esas komisyona görüş bildiren komisyona ise tali komisyon denmektedir. Teklif Meclis Başkanlığınca esas komisyon olarak Milli Savunma Komisyonuna havale edilirken, tali Komisyon olarak Adalet Komisyonu, Plan ve Bütçe Komisyonu ile Sanayi, Ticaret, Enerji, Tabi Kaynaklar, Bilgi ve Teknoloji Komisyonu belirlenmiştir. Hal böyle olunca teklif sahiplerince "Çatı bir mevzuat" olarak nitelendirilen teklifin öncelikle içinde barındırdığı kişisel verilerin ve ticari sırların işlenmesi ayrıca bu bilgilerin silinmesi, yok edilmesi, anonim

hale getirilmesine ilişkin hükümler dolayısı ile Adalet Komisyonunda ve hatta hiç havalesi yapılmayan Anayasa Komisyonunda görüşülmesi gerekmektedir.

Konu yukarıda ayrıntılı olarak arz ve izah edildiği üzere doğrudan Anayasa ile korunan haklara ilişkindir. Yaşanması muhtemel hak ihlallerinin tespiti ve önlenmesi amacıyla etkin ve yerinde bir çalışma Anayasa Komisyonunun ihtisas alanındadır. Nihayetinde Anayasa Mahkemesinin de kişisel verilerin işlenmesi, depolanması ve imhasında yaşanılan hukuka aykırılıklara yönelik sayısız kararı bulunmaktadır. Bu açıdan teklifin Meclis Başkanlığınca Anayasa Komisyonuna havalesinin yapılmamış olması esası etkileyen bir usul hatasıdır.

Özellikle üzerinde durulması gereken bir diğer husus ise TBMM İç Tüzüğüne göre kurulmuş ihtisas komisyonlarından biri olan Güvenlik ve İstihbarat Komisyonuna kanun teklifinin hiç havalesinin yapılmamış olmasıdır. Komisyon hakkında detay araştırıldığında; Milli güvenliğe ilişkin konularda görüş ve öneriler sunmak, güvenlik ve istihbarat konularında uluslararası alanda kabul gören gelişmeleri izlemek, güvenlik ve istihbarat hizmetleri sırasında elde edilen kişisel verilerin güvenliğini ve bireyin hak ve özgürlüklerini koruyucu öneriler geliştirmenin komisyonun görevleri arasında sayıldığı görülmüştür. Dolayısıyla siber güvenliğin sağlanması amacıyla hazırlanan, stratejik öneme sahip bu kanun teklifinin Güvenlik ve İstihbarat Komisyonunda görüşülmesi gerekmektedir. Teklifin komisyonda görüşülmesi şöyle dursun tali komisyon olarak bile havalesi yapılmamıştır.

Unutulmamalıdır ki yasa yapım sürecinde komisyon görüşmelerine ihtiyaç duyulmasının temel sebebi inceleme aşamasına zaman ayrılması ve tekliflerin uzman ekipler tarafından tüm boyutları ile dikkatle incelenmesidir. Mevcut iktidar partisi sahip olduğumuz bu gücü de işlevsiz hale getirerek, kanun tekliflerinin sarayda hazırlanan metinlerden ileri gidememesine sebep olmuştur.

Yasama organındaki çoğunluğuyla, iktidarın kendi politik çıkarları doğrultusunda kanunlaşan teklif, amaç unsuru bakımından sakatlıklar barındırmaktadır. Oysa yasaların temel amacı toplumun gereksinimlerine zamanında ve yeterince cevap vermek ve kamu yararını gözetmek olmalıdır.

3. Müzakere Eksikliği:

Değinmek istediğimiz bir diğer husus ise kanun tekliflerinin komisyonlarda görüşülmesi sırasında, muhalefet partilerinin öneri ve eleştirilerinin göz ardı edilmesidir. Yasama sürecinde, muhalefet partilerinin öneri ve eleştirilerinin göz ardı edilmesi, demokratik katılımcılığı

zedelemekte ve bu sürecin tek taraflı işlemesine yol açmaktadır. Özellikle siber güvenliğin sağlanmasına hizmet edecek bu kanunda muhalefet partilerinin yanı sıra ayrıca bu kanun kapsamına alınan kurum ve kuruluşlar ile gerçek ve tüzel kişilerden oluşan heyetlerin dinlenmesi ve mümkünse katkı sağlamaları gerekmektedir. Teknik donanım, teknolojik yeterlilik gibi hususların ise ayrıca değerlendirilmesi gerekmektedir.

Ülkemizde yasa yapımı hükümet politikalarını uygulama aracı olarak kullanılmaktadır. Gazi Meclis özellikle son iki döneminde ağırlıklı olarak KHK ve CBK'ların düzenleyemeyecekleri alanlara müdahale etmesi sonucu AYM iptal kararları neticesinde faaliyet göstermektedir. Yasama toplumun ihtiyaçlarının tespit edilip düzenlenmesinden çok mevcut iktidarın ve iktidar yanlılarının taleplerine göre şekillenmektedir. Kamu yararı gözetilmeden kişisel ve siyasal ikbal uğruna hazırlanan tekliflerin kanunlaştırılmak istendiğine şahit olunmaktadır.

Çağın bir gereği olarak gördüğümüz ve teklif sahiplerinin de bu şekilde gerekçelendirdiği yasa içeriğe bakıldığında bir hayli problemli görünmektedir. Muhalefetin ve komisyona katılan diğer katılımcıların yapıcı eleştirilerinin dikkate alınmadığı göstermelik değişimlerle teklife müdahale edildiği anlaşılmaktadır. Ancak bu değişiklikler de tatmin edici değildir.

Yeterli hazırlık aşamasından geçmemiş, kapsamlı bir kanun için gerekli olan ilkelere uyulmamış, ilgili çevrelerin ve profesyonel ekiplerin katılmadığı, hızlı bir şekilde kanunlaşıp yürürlüğe girmiş kurallar uygulama sürecinde sayısız hukuka aykırı işleme ve hak ihlaline sebebiyet verdiğinden AYM tarafından iptal edilmekte ve Gazi Meclis bu kanunlardaki eksikliği gidermeye çalışmaktadır.

Yasama süreci yani hukuk yaratmak açık, şeffaf ve hesap verilebilir ilkeler doğrultusunda yapılmalıdır. Kanunlaşma süreci kamuya açık olmalıdır. Milli Güvenlik Komisyonunda görüşülen Siber Güvenlik Kanun Teklifinde ise bu ilkelerin hiçbiri göz önünde bulundurulmamış ve süreç alelacele bitirilmeye çalışılmıştır.

GENELİ ÜZERİNE DEĞERLENDİRMELERİMİZ

Dijital teknolojilerin hayatın her alanında giderek daha fazla yer alması, bireylerden devletlere kadar herkesin dijital sistemlere bağımlı hale gelmesine yol açmıştır. Bu durum, siber güvenliği sadece teknolojik bir gereklilikten çıkarıp, ulusal güvenliğin temel yapı taşlarından biri haline getirmiştir.

Askeri ve istihbarat operasyonları, siber saldırılara karşı savunmasız olan kritik altyapılara (enerji, su, ulaşım, finansal sistemler vb.) yönelik siber tehditler nedeniyle büyük risk altına girebilmektedir. Bu tehditler, devletin ekonomik, sosyal ve siyasi istikrarını doğrudan etkileyebilmektedir.

Günümüzde siber güvenlik, geleneksel askeri stratejilerin yerini alabilecek bir alan olarak yükselmiştir. "**Siber savaş**" fiziksel çatışmalara gerek kalmadan, bir ülkenin dijital altyapılarına yapılan saldırılarla önemli zafiyetler yaratılmasını mümkün kılmaktadır. Bilgi güvenliği, sadece devletin değil, aynı zamanda vatandaşların da korunmasını sağlayan bir temel unsurdur. Bu doğrultuda; ülkelerin siber güvenlik kapasitesi, vatandaşın güvenliği ile de doğrudan ilişkilidir ve "**siber savunma"** geleneksel askeri savunmalar kadar önemli hale gelmiştir.

Dijital teknolojilerin yaygınlaşması suç tanımlarına da yeni kavramlar eklenmesine neden olmuştur. Devletin gizli belgelerine yönelik yapılan saldırıları ifade eden "dijital casusluk" ve özel şirket ve kişileri de tehdit altında bırakan "bilgi hırsızlığı" ülkeleri, siber güvenlik suçlarının önlenmesi, kritik altyapıların güvenliği konusunda sıkı tedbirler almak zorunda bırakmıştır.

Kanun teklifinin gerekçesinde yer aldığı üzere, 2024 yılında Uluslararası Telekomünikasyon Birliği tarafından Siber Güvenlik Endeksi yayınlanmış, "Rol Model Ülke" kategorisi içinde yer alan 46 ülkenin siber güvenlik yapısı ve mevzuatı incelenmiştir. Siber Güvenlik Endeksi verilerine göre, bu ülkelerin yaklaşık yüzde 91'inin kapsamlı bir çatı mevzuatına sahip olduğu, ülkemizin ise "Rol Model Ülke" kategorisinde yer almasına rağmen gerçek anlamda çatı mevzuat özelliği teşkil edecek kapsamlı bir siber güvenlik kanununun eksikliğine yer verilmiştir.

Ülkemizde siber güvenliğe yönelik politikalar 2013 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile şekillendirilmeye başlansa da bu strateji, zaman içinde dijital dünyadaki hızlı değişimlere ve gelişen tehditlere karşı yeterince güncellenmemiştir. Güvenlik stratejilerinin yeterince gelişmemiş olması ve hızla değişen tehdit ortamı Türkiye'nin karşılaştığı risklerin büyümesine neden olmaktadır. Bu nedenle Siber Güvenlik alanında bir yasal düzenlemenin yapılması aciliyet gerektiren bir durum olarak ortaya çıkmaktadır. İYİ Parti olarak, siber güvenlik alanındaki bu kanun teklifini, geç kalmış bir düzenleme olarak

destekliyoruz ancak çekincelerimizi de dikkate alarak daha geniş kapsamlı bir yaklaşım benimsenmesi gerektiğini düşünüyoruz.

Bu doğrultuda kanun teklifinin hem komisyon öncesi bilgilendirme toplantısında hem de komisyon görüşmeleri sırasında önceliklerimizi ve çekincelerimizi bildirmiş, kanun teklifinin özellikle devlet güvenliğini ilgilendiren hassas maddeleri konusundaki itirazımız dile getirilmiştir.

Özelikle kanun teklifinin 2. maddesi ile Siber Güvenlik Kanununun kapsamı dışında bırakılan alanda sadece Millî İstihbarat Teşkilâtı, Emniyet Genel Müdürlüğü ve Jandarma Güvenlik Komutanlığının yürüttüğü faaliyetler bulunmaktayken İYİ Parti olarak itirazlarımız neticesinde, Türk Silahlı Kuvvetleri ve Sahil Güvenlik Komutanlığının da bu kanundan istisna tutulan kurumlar arasında yer alması sağlanmıştır.

Kanun teklifi hazırlanırken ülkemizin 2016 yılında FETÖ tarafından yapılan hain darbe girişimi ve yine 2009 yılının aralık ayında başlayan 20 gün süren "Kozmik Oda"ya girilmesi ihanetleri göz ardı edilmiştir. Teklif hazırlanırken bu hususlara dikkat edilmemesinin büyük bir eksiklik olduğu İYİ Parti tarafından hatırlatılmış, Türk Silahlı Kuvvetleri ve Sahil Güvenlik Komutanlığının da kanun kapsamı dışında bırakılmasında ısrarcı olunmuştur. Ancak AK Parti bizim uyarılarımız sonucu hazırladığı bu önergeyi yalnızca kendi üyeleri ile imza altına almıştır.

2016 yılı sonrası yapılan yargılamalarla da ispat olunduğu üzere FETÖ tarafından planlı bir şekilde Seferberlik Daire Başkanlığı'na girilmesi, sadece bir güvenlik ihlali değil, aynı zamanda Türkiye'nin iç siyaseti ve güvenlik sisteminin ne kadar hassas ve kırılgan olduğunu gösteren acı bir tecrübedir. Bununla birlikte bu kanun teklifi hazırlanırken Türkiye'nin ulusal güvenliğine yönelik ihanetin göz ardı edilmesi, hükümetin bu olaylardan ders almadığının bir göstergesi olarak karşımıza çıkmaktadır.

Kanun teklifi ile, 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 Kurulu'nun kurulmasına ilişkin esaslar düzenlenmektedir.

Teklifle, Siber Güvenlik Başkanlığı kurulmakta, 'Barındırma', 'Başkan', 'Başkanlık', 'Bilişim sistemleri', 'Kritik altyapı', 'Kritik kamu hizmeti', 'Siber güvenlik', 'Siber olay', 'Siber saldırı', 'Siber tehdit', 'Siber tehdit istihbaratı', 'Siber uzay', 'SOME', 'Varlık' ve 'Zafiyet'in tanımları yapılmakta ve siber güvenliğin sağlanmasındaki temel ilkeler belirlenmektedir.

Teklife göre Siber Güvenlik Başkanlığı, ilgili mevzuatta yer alan görevlerin yanı sıra 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 yürütecektir.

Siber Güvenlik Kanun teklifi, Türkiye'de dijital güvenliği sağlamaya yönelik yasal düzenlemeleri içerse de AK Parti iktidarının yıllar içerisinde ifade özgürlüğünün kullanılmasına ilişkin uygulamaları, vatandaşın, gazetecilerin dijital ortamda izlenmesine ve kişisel verilerin gizliliğinin tehlikeye atılabileceği endişesini de beraberinde getirmiştir.

Kanun teklifinde yer alan "kritik altyapı" ve "siber güvenlik" tanımının geniş ve belirsiz olması, "tüzel kişiliği bulunmayan kuruluşlar" ifadesinden ne kastedildiği gibi hususların açıklıkla ifade edilmemesi, teklifin 16. Maddesinin 5. Fıkrasında yer alan "siber uzayda veri sızıntısı olmadığı halde algı oluşturmak suretiyle kurumları ve şahısları hedef almaya yönelik faaliyet yürütenlere" ibaresinin kişisel verilerin korunması ve özel hayatın gizliliği ile aynı zamanda ifade özgürlüğü üzerinde ciddi kısıtlamalar yaratabilecek olması hususlarında İYİ Parti gereken uyarıları yapmıştır. Madde, komisyonda "Siber uzayda veri sızıntısı olmadığı halde halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef almak amacıyla veri sızıntısı yapılmış gibi içerik oluşturanlara ve/veya bu içerikleri yayanlara iki yıldan beş yıla kadar hapis cezası verilir" şeklinde değiştirilse de, siber güvenlik politikaları dengeli bir yaklaşım gerektirdiği için yalnızca güvenlik önlemlerini artırmak değil, aynı zamanda bireysel hakları ve özgürlükleri koruyarak uygulanması gerektiği konusundaki hassasiyetimiz devam etmektedir.

MADDELER ÜZERİNE DEĞERLENDİRMELERİMİZ

MADDE 1, MADDE 2, MADDE 6, MADDE 7

"tüzel kişiliği bulunmayan kuruluşlar" Kavramının Belirsizliği (1,2,6 ve 7. Maddeler üzerine değerlendirmemiz)

Teklifin 1 inci maddesinde kanunun amacı kısmında tüzel kişiliği bulunmayan kuruluşlarında siber saldırılara karşı korunacağı düzenlenmek istenmektedir. Gerek kamu idareleri gerekse kamu kurumları birer kamu tüzel kişisidir ve kamu tüzel kişilerinin sahip olduğu ortak özelliğe sahiptirler. Teklif metninden kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunacağı kanunun niteliği gereği anlaşılabilmektedir. Ancak tüzel kişiliği bulunmayan kuruluşlar ifadesinden ne kast edildiği ve kimlerin korunacağı anlaşılamamaktadır.

Teklifte yer alan 2. madde ile kanunun kapsamı düzenlenmektedir. Bu maddenin birinci fıkrasında kamu kurum ve kuruşları, meslek kuruluşları, gerçek ve tüzel kişiler kapsam dahilinde tutulurken ayrıca bir de tüzel kişiliği bulunmayan kuruluşların kapsama alınması yerinde değildir. Anlaşılır olmayan oluşumların kapsama alınması kamu kurumlarının bu belirsiz oluşumları muhatap alması anlamına gelecektir ve bu idare hukukunun temel ilkeleriyle çelişmektedir.

Aynı şekilde teklifin 6. maddesinde başkanlığın yetkileri düzenlenmektedir. Maddenin g bendinde tüzel kişiliği bulunmayan kuruluşların sınıflandırılması yapılmaktadır. Bu durumda benzer bir şekilde belirsizlik içermektedir.

7. Maddede de "tüzel kişiliği bulunmayan kurum ve kuruluşlar" iş birliği açısından kapsama alınmıştır. Anayasanın 123'üncü maddesi kapsamında kamu tüzel kişilikleri idarenin bütünlüğü ilkesi korunarak merkezden yönetim ve yerinden yönetim esasları çerçevesinde oluşturulmuştur. Yani merkezi idarenin ve yerinden yönetim idarelerinin kamu tüzel kişilikleri bulunmaktadır. Bu çerçevede maddenin ikinci fıkrasında iş birliği içerisinde çalışılacaklar arasında kamu kurum ve kuruluşları denilerek tüm kamu tüzel kişilikleri ve merkezi idare dışında kamu tüzel kişiliği olmayan kamu idareleri kastedilmektedir. Aynı fıkrada gerçek ve tüzel kişiler de iş birliği yapılacaklar arasında sayılmıştır.

Hukuk devleti ilkesi, kanunların açık, anlaşılır ve kesin bir şekilde düzenlenmesini gerektirir. Ancak "tüzel kişiliği bulunmayan kuruluşlar" kavramı, Türk hukuk sisteminde hukuki belirsizliğin adeta somutlaşmış bir örneği olarak karşımıza çıkmaktadır. Bu kavramın tanımlanmadan ve sınırları belirlenmeden kullanılması hem hukuk sistemine hem de bireylerin temel haklarına doğrudan zarar veren ciddi bir eksikliktir.

Bir hukuk düzeninde kullanılan kavramların açık ve net olmaması, hukuki güvenlik ilkesinin ağır bir şekilde ihlalidir. "Tüzel kişiliği bulunmayan kuruluşlar" kavramı, içeriği tanımlanmadığı için bireyler ve kurumlar açısından hangi oluşumların bu kapsamda değerlendirileceğini öngörmeyi imkânsız hale getirmektedir. Hukuki düzenlemelerin belirsiz olması, vatandaşların ve kuruluşların davranışlarını hukuk düzenine uygun şekilde planlamasını engeller. Bu durum, yalnızca hukuki güvenlik ilkesini değil, aynı zamanda hukuk devleti ilkesinin temel yapı taşlarını da sarsmaktadır. Bu tür bir belirsizlik, hukuk sistemini keyfiliğe açık hale getirmekte ve hukuk normlarına duyulan güveni zedelemektedir.

Sonuç olarak, "tüzel kişiliği bulunmayan kuruluşlar" kavramının açık bir şekilde tanımlanması ve kapsamının sınırlarının netleştirilmesi gerekmektedir. Bu belirsizlik giderilmediği sürece, hukuki güvenlik, eşitlik ve öngörülebilirlik ilkeleri zarar görecek; idarenin keyfi uygulamalarına açık bir alan bırakılacaktır.

Türk Silahlı Kuvvetlerinin Kanunun Kapsamı Dışında Bırakılmaması (2. Madde üzerine değerlendirmemiz)

Teklifte yer alan 2 inci madde ile kanunun kapsamı düzenlenmiş, maddenin ikinci fıkrasında ise kanunun kapsamı dışında bırakılan istihbari faaliyetler belirlenmiştir. Ancak Türk Silahlı Kuvvetleri (TSK), kanunun kapsamı dışında bırakılan kurumlar arasında sayılmamıştır. Bu durum, ordumuzun gizli bilgilerinin ifşa edilmesi riskini beraberinde getirmekte ve ulusal güvenliğimizi tehdit edebilecek ciddi bir hukuki zafiyet yaratmaktadır. Daha önce yaşanan acı tecrübeler, bu tür risklerin gerçekleşmesi halinde ortaya çıkacak tehlikenin büyüklüğünü açıkça göstermektedir.

Nitekim 2009 yılında kamuoyunda "kozmik oda" olarak bilinen Genelkurmay Ankara Seferberlik Bölge Başkanlığı'nda yapılan 20 gün süren aramalar, Türk Silahlı Kuvvetleri'nin devlet sırrı niteliğindeki belgelerinin FETÖ mensuplarınca ele geçirilmesiyle sonuçlanmıştır. Bu süreçte, ulusal güvenliğe ilişkin en kritik bilgiler deşifre edilmiş, daha sonra bu gizli bilgilere erişimde rol oynayan kişilerin sanık olarak yargılandığı davalarda Yargıtay Ceza Genel Kurulu

tarafından "silahlı terör örgütüne üye olmak" ve "devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri casusluk amacıyla açıklamak" suçlarından verilen cezalar onanmıştır.

Yargıtay'ın bu davada dayandığı raporda, "Devlet sırrı olduğu belirtilen bir kısım belgelerin, düşman ülkeye savaş hazırlıklarımızı, savaş etkinliğimizi ve çalışma prensiplerimizi ortaya koyabilecek nitelikte bilgiler içerdiği" açıkça tespit edilmiştir. Bu durum, ulusal güvenliğe yönelik böylesi hassas bilgilerin ifşa edilmesinin ne denli ağır sonuçlar doğurabileceğini bir kez daha ortaya koymuştur.

Söz konusu teklifte, Türk Silahlı Kuvvetleri'nin istihbari faaliyetlerinin kapsam dışında bırakılmaması benzer olayların tekrar yaşanması riskini artıracaktır. Ulusal güvenliğimizin temelini oluşturan TSK'nın stratejik ve istihbari bilgilerinin bu şekilde risk altında bırakılması kabul edilemez bir durumdur. Ülkemizin güvenliği açısından TSK'nın gizli ve kritik faaliyetlerinin hiçbir şekilde açık edilmemesi ve bu kapsamda söz konusu kanun teklifinde TSK'nın istihbari faaliyetlerinin de açıkça kanun kapsamı dışında bırakılması zorunludur. Nitekim komisyon sürecindeki yoğun muhalefetimiz sonucu Türk Silahlı Kuvvetleri kanun kapsamı dışında bırakılmıştır.

Kişisel Verilerin Anonim Hale Getirilmesi (6. Madde üzerine değerlendirmemiz)

Kişisel Verileri Koruma Kurumu, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerini düzenleyen rehberinde anonim hale getirme işlemini, "kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi" şeklinde tanımlamıştır. Anonim hale getirme işleminin başarıyla tamamlanmış sayılabilmesi için, kişisel verilerin, veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ya da başka verilerle eşleştirilmesi gibi yöntemlerle dahi kimliği belirlenebilir bir kişiyle ilişkilendirilemeyecek hale getirilmesi gerekmektedir. Bu süreç, manuel işlemlerle, otomatik sistemlerle veya her iki yöntemin birleşiminden oluşan melez işlemlerle gerçekleştirilebilmektedir. Ancak kritik olan nokta, anonim hale getirilmiş verilerin paylaşıldıktan veya ifşa edildikten sonra, bu verilere erişebilen veya sahip olan yeni kullanıcılar tarafından anonimliğin bozulmasını engelleyecek önlemlerin alınmasıdır.

Teklifin 6. maddesi ile kanunda belirtilen yetkiler çerçevesinde elde edilecek kişisel veriler ve ticari sırların, bu verilere erişilmesini gerektiren sebeplerin ortadan kalkması halinde

resen silinip, yok edilip veya anonim hale getirileceği düzenlenmektedir. Maddenin lafzına göre, bu uygulamaya ilişkin usul ve esaslar Cumhurbaşkanı tarafından çıkarılacak bir yönetmelikle belirlenecektir. Ancak tüm dijital verilere ve belgelere erişim yetkisine sahip bu denli kritik bir başkanlıkta anonim hale getirmenin taşıdığı riskler göz ardı edilemeyecek kadar büyüktür.

Anonim hale getirme işlemi, teknik açıdan karmaşık bir süreç olup yanlış yöntemler kullanıldığında veya yeterli önlemler alınmadığında anonimliğin bozulma riski oldukça yüksektir. Kişisel verilerin anonim hale getirildikten sonra dahi çeşitli teknikler kullanılarak tekrar kimliği belirlenebilir hale getirilebildiği bilimsel olarak kanıtlanmıştır. Bu durum, kişisel verilerin korunması açısından telafisi mümkün olmayan zararlar doğurabilir. Özellikle devletin kritik birimlerinde ve yüksek güvenlik gerektiren başkanlıklarda bu tür risklerin kabul edilmesi mümkün değildir.

Ayrıca, teklifin uygulama usul ve esaslarının yönetmelikle düzenlenecek olması, anonim hale getirme işleminin nasıl yapılacağına ilişkin belirsizlik yaratmaktadır. Anonimleştirme gibi teknik bir sürecin yeterince şeffaf ve denetlenebilir olmaması, bu süreçte yapılacak hataların sonuçlarını daha da ağırlaştırabilir. Bu durum, yalnızca kişisel verilerin güvenliğini tehlikeye atmakla kalmayacak, aynı zamanda ticari sırların ifşa edilmesine de neden olabilecektir.

Bu riskler göz önünde bulundurulduğunda, kişisel verilerin anonim hale getirilmesi yerine, bu verilere erişim gerektiren sebeplerin ortadan kalkması durumunda söz konusu verilerin silinmesi veya yok edilmesi daha güvenli ve uygun bir çözüm olacaktır. Silme veya yok etme işlemleri, verilerin tekrar erişilebilir hale getirilmesini önlemek açısından daha kesin ve güvenli bir yöntemdir.

MADDE 15

Müsadere, hukuki niteliği gereği bir güvenlik tedbiri olarak Türk Ceza Kanunu'nun 54. ve 55. maddelerinde düzenlenmiştir. Eşya müsaderesi, suça konu olan eşyanın mahkeme kararıyla mülkiyetinin kamuya geçirilmesini sağlamaktadır.

Teklifin mevcut haliyle yasalaşması durumunda, suça ilişkin kesin hüküm olmadan müsadere edilen eşya veya kazancın Başkanlığa geçici olarak tahsis edilmesi veya bedelsiz devredilmesi, mülkiyet hakkının ağır bir şekilde ihlali anlamına gelecektir. Anayasa'nın 35.

maddesi ile güvence altına alınan mülkiyet hakkı, ancak kanunun öngördüğü sınırlar ve usuller çerçevesinde kısıtlanabilir. Ancak teklif, bu sınırları aşarak mülkiyet hakkını zedelemekte ve hukukun temel ilkelerine aykırı bir düzenleme getirmektedir.

Müsadere kararı, ceza yargılamasının bir sonucudur. Teklifte öngörülen şekilde suça ilişkin kesinleşmiş bir mahkeme kararı olmaksızın eşyanın müsadere edilmesi ve bu müsadere edilen malların kamu kurumlarına devredilmesi, hukuk devleti ilkesiyle bağdaşmayan ağır bir hak ihlali teşkil edecektir. Ceza hukukunda masumiyet karinesi, kesin hüküm sağlanana kadar kişilerin suçlu kabul edilemeyeceğini öngörmektedir. Ancak teklifin bu haliyle uygulanması, masumiyet karinesinin ihlal edilmesine ve henüz suçluluğu kesinleşmemiş bireylerin malvarlıklarının hukuka aykırı şekilde tasarrufa konu edilmesine yol açacaktır.

Ayrıca, teklif ile düzenlenen "müsadere edilen mal veya kazancın Başkanlığa geçici olarak tahsis edilmesi" ya da "bedelsiz devredilmesi" gibi hükümler, mülkiyet hakkının ihlali yanında, ceza hukukunun temel prensipleri olan orantılılık ve hukuki belirlilik ilkelerini de açıkça ihlal etmektedir. Mülkiyet hakkı, yalnızca suçla bağlantısı kesin olarak tespit edilen malların hukuki bir karar neticesinde müsadere edilmesiyle sınırlandırılabilir. Ancak, teklifin öngördüğü düzenleme, bu temel hukuki prensibi yok saymakta ve keyfi uygulamalara zemin hazırlamaktadır.

Bu düzenleme, yalnızca bireylerin mülkiyet hakkını değil, aynı zamanda yargı kararlarının bağlayıcılığını ve yargı bağımsızlığını da zedelemektedir. Ceza yargılaması süreci tamamlanmadan mülkiyetin kamuya geçirilmesi, yargı kararlarını etkisizleştirebilecek bir müdahale anlamına gelir. Bu durum, hukuk devletine olan güveni zedeleyecek ve mülkiyet hakkı ile masumiyet karinesini ihlal ederek temel hak ve özgürlüklerin korunması açısından ciddi sorunlara yol açacaktır.

MADDE 16

Teklifte yer alan madde ile cezai hükümler düzenlenmektedir. Teklifin 16 ıncı maddesinin beşinci fıkrasının ilk halinde ise "veri sızıntısı olmadığı halde veri sızıntısı yapılmış gibi algı oluşturma suretiyle kurumları veya şahısları hedef alma" suçu tanımlanmıştır. Ancak bu düzenlemede yer alan "algı oluşturma" ve "kurumları ya da şahısları hedef alma" ifadeleri son derece muğlak olup suçun unsurları net bir şekilde tanımlanmamıştır.

Bu fıkrada yer alan suçun oluşması için, bir veri sızıntısı iddiasının gerçekten algı oluşturmak amacıyla mı yapıldığı veya bu iddianın kurumları ya da şahısları hedef alacak şekilde mi olduğu, uygulamada objektif ve somut biçimde tespit edilmesi neredeyse imkânsızdır. Söz konusu düzenleme, soyut ve yoruma açık ifadeler içermesi nedeniyle keyfi uygulamalara açık bir zemin hazırlamaktadır. Bu belirsizlik, iktidarın sıkça yaptığı gibi yargının bir baskı aracı olarak kullanılmasına neden olabilecek ciddi riskler taşımaktadır.

Bu düzenleme, Türk Ceza Kanunu'na 7418 sayılı kanunun 29. maddesi ile eklenen "Halkı yanıltıcı bilgiyi alenen yayma" başlıklı 217/A maddesi ile benzer bir nitelik taşımaktadır. Söz konusu 217/A maddesi, düzenlenirken İYİ Parti ve diğer muhalefet partilerinin yoğun eleştirilerine maruz kalmış, ancak bu eleştiriler dikkate alınmaksızın Cumhur İttifakı oylarıyla kabul edilmiştir. 217/A maddesi, basın özgürlüğüne yönelik tehdit oluşturmuş, özellikle muhalif gazeteciler, medya mensupları ve sosyal medya kullanıcılarının sindirilmesi için bir araç haline getirilmiştir.

Teklifin 16. maddesinin beşinci fıkrasının ilk hali de aynı şekilde başta muhalif gazeteciler, medya mensupları ve sosyal medya kullanıcıları olmak üzere, tüm muhalif vatandaşları baskı altına almayı hedefleyen bir düzenleme niteliğindedir. "Algı oluşturma" veya "kurumları/kişileri hedef alma" gibi subjektif değerlendirmelere dayalı ifadeler, muhaliflerin hukuka aykırı şekilde cezalandırılmasına yol açabilecek ciddi mağduriyetlere neden olacaktır. Özellikle habercilik ve basın faaliyetleri bu madde kapsamında yanlış yorumlanarak cezalandırılma riski taşımaktadır. Basın mensupları tarafından yapılan eleştirel haberler, sırf iktidarın hoşuna gitmediği için "algı oluşturma" bahanesiyle cezai yaptırımlara tabi tutulabilecektir.

İlgili fıkra komisyon aşamasında iktidar partisince değiştirilmiş, veri sızması hakkında içerik oluşturmanın "halk arasında endişe, korku, panik yaratmak" ve "kurumları ve şahısları hedef almak amacıyla" yapılması durumunda 2 yıldan 5 yıla kadar hapis cezası öngörülmüştür. Bu değişiklik bizim yukarıda bahsettiğimiz çekincelerimizi gidermekte yetersiz kalmıştır. Kanun uygulayıcılarına adeta bir "niyet okuma" hakkı tanınmıştır. Söz konusu değişiklikle bile teklif, kanunilik ilkesini karşılamamaktadır. Açık ve anlaşılır olmadığı gibi insanların amaçlarına dair niyet okuma yetkisi getirilmektedir. Kimin neyi ne niyetle yaptığı ancak kesin delillerle belirlenebilir. Başka türlü amacın ne olduğunun belirlenebilmesi mümkün değildir.

Bu düzenleme, Anayasa'nın 26. maddesi ile güvence altına alınan ifade özgürlüğüne ve 28. maddesi ile koruma altına alınan basın özgürlüğüne açıkça aykırıdır. Ayrıca, Avrupa İnsan Hakları Sözleşmesi'nin 10. maddesinde yer alan ifade özgürlüğü hakkının ihlali anlamına gelecektir. Bu tür düzenlemeler, demokratik bir hukuk devletinde asla kabul edilemez.

Teklifin 16. maddesinin beşinci fıkrası, ifade özgürlüğü ve basın özgürlüğü üzerinde ciddi bir baskı yaratacak, yargının siyasi saiklerle kullanılması riskini artıracak ve muhalif kesimleri susturmayı hedefleyen bir araç haline gelecektir. Bu nedenle, yukarıda detaylı olarak açıklanan gerekçelerle, söz konusu fıkranın madde metninden çıkarılması elzemdir. Bu düzenlemenin yasalaşması halinde doğacak hukuki ve toplumsal mağduriyetlerin telafisi mümkün olmayacaktır.

Sonuç olarak;

Teklifi ihtiyaç duyulan bir kanun teklifi olması nedeniyle destekliyoruz. Ancak; yukarıda detaylarıyla anlatılan gerekçeler sebebiyle bazı maddelerin eksik olduğu ya da olumsuz etki yaratacağını vurguluyor ve bu eksikliklerin Genel Kurul'da düzeltilmesi gerektiği kanaatini taşıyoruz. Dolayısıyla 2/2860 esas numaralı Siber Güvenlik Kanunu Teklifine dair çekincelerimizi dikkate sunarız.

Ayyüce Türkeş Taş
Adana

Adnan Şefik Çirkin
Hatay

AFYONKARAHİSAR MİLLETVEKİLİ ALİ ÖZKAYA VE ANTALYA MİLLETVEKİLİ ATAY USLU İLE 131 MİLLETVEKİLİNİN TEKLİFİ	MİLLÎ SAVUNMA KOMİSYONUNUN KABUL ETTİĞİ METİN
SİBER GÜVENLİK KANUNU TEKLİFİ	**SİBER GÜVENLİK KANUNU TEKLİFİ**
BİRİNCİ BÖLÜM	**BİRİNCİ BÖLÜM**
Başlangıç Hükümleri	**Başlangıç Hükümleri**
Amaç	**Amaç**
MADDE 1- (1) Bu Kanunun amacı, Türkiye Cumhuriyetinin 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.	**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	**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.	**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 Salahiyet Kanununun ek 7 nci maddesi ve 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun ek 5 inci maddesi uyarınca yürütülen istihbari faaliyetler ile 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu uyarınca yürütülen faaliyetler bu Kanun kapsamı dışındadır.	(2) 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet 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 uyarınca yürütülen faaliyetler bu Kanun kapsamı dışındadır.
Tanım ve kısaltmalar	**Tanım ve kısaltmalar**
MADDE 3- (1) Bu Kanunda geçen;	**MADDE 3-** (1) Bu Kanunda geçen;
a) Barındırma: Bilişim sistemlerinin harici bir veri merkezinde bulundurulmasını,	a) Barındırma: Bilişim sistemlerinin harici bir veri merkezinde bulundurulmasını,
b) Başkan: Siber Güvenlik Başkanını,	b) Başkan: Siber Güvenlik Başkanını,
c) Başkanlık: Siber Güvenlik Başkanlığını,	c) Başkanlık: Siber Güvenlik Başkanlığını,

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
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,	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,	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,	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,	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 bu sistemler tarafından işlenen verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini,	g) Siber olay: Bilişim sistemlerinin veya bu sistemler tarafından işlenen 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,	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,	h) Siber tehdit: Bilişim sistemlerinin, bu sistemlerde bulunan veya bu sistemler tarafından işlenen verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesine neden olabilecek potansiyel tehlikeleri,

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

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.

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

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.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

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

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

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

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
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.	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.	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.	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.	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.	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.	h) Siber güvenlik denetimini gerçekleştirmek ve sonucuna göre yaptırım uygulamak.
i) 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.	i) 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.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
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 alt yapısından 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.	**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.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

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 smıflandırabilir, 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 kullanım öncesinde uygunluk verir.

i) 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

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

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 kullanım öncesinde uygunluk verir.

i) 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

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
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.	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.	(3) Bu maddenin uygulanmasına ilişkin usul ve esaslar Cumhurbaşkanı tarafından çıkarılacak yönetmelikle belirlenir.
Sorumluluklar ve iş birliği	**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:	**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.	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.	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 uzmanları ve şirketlerden tedarik etmek.	c) Kamu kurumları ve kuruluşları ile kritik altyapılarda kullanılacak siber güvenlik ürün, sistem ve hizmetleri Başkanlık tarafından yetkilendirilmiş ve belgelendirilmiş siber güvenlik uzmanları ve şirketlerden tedarik etmek.
ç) Sertifikasyon, yetkilendirme ve belgelendirmeye tabi siber güvenlik şirketlerince faaliyete başlamadan önce mevcut düzenlemeler çerçevesinde Başkanlığın onayını almak.	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 tavsiye ve benzeri belgelerde yer alan hususları yerine getirmek ve gerekli tedbirleri almak.	d) Siber olgunluğun artırılmasına yönelik Başkanlık tarafından geliştirilen politika, strateji, eylem planı ile yayımlanan tavsiye ve benzeri belgelerde 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.	(2) Başkanlık, bu Kanunda belirtilen faaliyetlerin yürütülmesinde kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşlarla iş birliği içerisinde çalışır.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

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 görüldüğü 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.

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

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.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
(5) Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Başkanın yazılı emri ile konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama yapılabilir ve kopya çıkarma ve elkoyma işlemi gerçekleştirilebilir. Hâkim kararı olmaksızın yapılan arama ve gerçekleştirilen kopya çıkarma ve elkoyma 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 elkoyma kendiliğinden kalkar. Bu fıkra kapsamına giren talepler bakımından Ankara sulh ceza hâkimliği yetkili ve görevlidir. Ancak kamu kurum ve kuruluşları bakımından hâkimlik kararı aranmaz.	(5) Millî güvenlik, kamu düzeni, suç işlenmesinin veya siber saldırıların önlenmesi amacıyla hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının veya Başkanın yazılı emri ile konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama yapılabilir ve kopya çıkarma ve el koyma işlemi gerçekleştirilebilir. 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. 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	**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.	**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.	(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.	(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.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

(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

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

(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

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
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.	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.	(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	**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.	**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	**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.	**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, Siber Güvenlik Başkanlığınca 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.	(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	**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	**MADDE 13-** (1) Başkanlık tarafından yürütülen görev ve faaliyetler kapsamında edinilen kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgiler, kişisel veriler, ticari sırlar

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

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 kat'i 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.

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

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 kat'i 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.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

(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 veya bu Kanundan kaynaklanan görev ve yetkilerini kötüye kullananlara 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 olmadığı halde veri sızıntısı yapılmış gibi bu yönde algı oluşturmak suretiyle kurumları veya şahısları hedef almaya yönelik faaliyet yürütenlere iki yıldan beş yıla kadar hapis cezası verilir.

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

(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 veya bu Kanundan kaynaklanan görev ve yetkilerini kötüye kullananlara 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 olmadığı halde halk arasında endişe, korku ve panik yaratmak ya da kurumları veya şahısları hedef almak amacıyla veri sızıntısı yapılmış gibi içerik oluşturanlara ve/veya bu içerikleri yayanlara iki yıldan beş yıla kadar hapis cezası verilir.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

(6) Türkiye Cumhuriyetinin 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) 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, yüz bin 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 %1'i ile vergi öncesi karının %20'sinden yüksek olanına kadar idari para cezası verilir.

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

(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) 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 %1'i ile vergi öncesi kârının %20'sinden yüksek olanına kadar idari para cezası verilir.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

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) Kamu destekleriyle kurulan, geliştirilen veya desteklenen siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerin yurt dışına satışı ile bunları üreten şirketlerin bölünme, birleşme, pay devri veya satış işlemleri,

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

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) Kamu destekleriyle kurulan, geliştirilen veya desteklenen siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerin yurt dışına satışı ile bunları üreten şirketlerin bölünme, birleşme, pay devri veya satış işlemleri,

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
Başkanlığın uygun görüşüne tabidir. Kamu kurum ve kuruluşları ile kritik altyapılar için yeni tedarik sözleşmeleri kapsamında kullanılacak siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerinin yurt dışına satışı ile bunları üreten şirketlerin bölünmesi, birleşmesi, pay devri veya satış işlemlerinin Başkanlık onayına bağlanmasına ilişkin usul ve esaslar Başkanlık tarafından belirlenir. Başkanlık, bu kapsamda yer alan ürün, sistem, yazılım, donanım ve hizmetler ve şirketlerle ilgili olarak kamu kurum ve kuruluşlarından bilgi ve belge talep edebilir.	Başkanlığın uygun görüşüne tabidir. Kamu kurum ve kuruluşları ile kritik altyapılar için yeni tedarik sözleşmeleri kapsamında kullanılacak siber güvenlik ürün, sistem, yazılım, donanım ve hizmetlerinin yurt dışına satışı ile bunları üreten şirketlerin bölünmesi, birleşmesi, pay devri veya satış işlemlerinin Başkanlık onayına bağlanmasına ilişkin usul ve esaslar Başkanlık tarafından belirlenir. Başkanlık, bu kapsamda yer alan ürün, sistem, yazılım, donanım ve hizmetler ve şirketlerle ilgili olarak kamu kurum ve kuruluşlarından bilgi ve belge talep edebilir.
(2) Birinci fıkraya ilişkin hususlar ve süreçler, Başkanlık tarafından çıkarılacak yönetmelikle belirlenir.	(2) Birinci fıkraya ilişkin hususlar ve süreçler, Başkanlık tarafından çıkarılacak yönetmelikle belirlenir.
Değiştirilen ve yürürlükten kaldırılan hükümler	**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.	**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."	"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) 5018 sayılı Kanuna ekli (II) sayılı Cetvelin "B) Özel Bütçeli Diğer İdareler" bölümüne aşağıdaki satır eklenmiştir.	(2) 10/12/2003 tarihli ve 5018 sayılı Kanuna ekli (II) sayılı Cetvelin "B) Özel Bütçeli Diğer İdareler" bölümüne aşağıdaki satır eklenmiştir.
"46) Siber Güvenlik Başkanlığı"	"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.	(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."	"(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;	(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.	a) 5 inci maddesinin birinci fıkrasının (h) bendi yürürlükten kaldırılmış ve (ı) bendi aşağıdaki şekilde değiştirilmiştir.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)

"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 ait ve münhasıran ulusal siber güvenlik faaliyetleri kapsamında kullanılan her türlü taşınır, bilgi işlem alt yapısı ve sistemler, taşıt, araç, gereç ve malzeme, fiziki ve elektronik ortamdaki her türlü kayıt ve doküman ile diğer her türlü varlık envanteri ile mezkur Başkanlıkça 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 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

(Milli Savunma Komisyonunun Kabul Ettiği Metin)

"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 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 Başkanlıkça 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 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

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
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.	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.
(3) Bilgi Teknolojileri ve İletişim Kurumu Başkanlığının 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.	(3) Bilgi Teknolojileri ve İletişim Kurumu Başkanlığının 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, bu Kanunun yayımından 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 Medeni 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.	(4) Siber güvenlik alanında faaliyet icra eden dernek, derneklerden oluşan federasyonlar, vakıflar ile ticaret şirketleri, bu Kanunun yayımından 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 Medeni 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.

(Afyonkarahisar Milletvekili Ali Özkaya ve Antalya Milletvekili Atay Uslu ile 131 Milletvekilinin Teklifi)	(Milli Savunma Komisyonunun Kabul Ettiği Metin)
(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.	(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.	(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.	**Yürürlük** **MADDE 20-** (1) Bu Kanun yayımı tarihinde yürürlüğe girer.
Yürütme **MADDE 21-** (1) Bu Kanun hükümlerini Cumhurbaşkanı yürütür.	**Yürütme** **MADDE 21-** (1) Bu Kanun hükümlerini Cumhurbaşkanı yürütür.

TBMM Basımevi - 2025