



**T.B.M.M.**

CUMHURİYET HALK PARTİSİ

Grup Başkanlığı

Tarih : 22 Haziran 2026

Sayı : 19474

46149

## TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞI'NA

Aşağıda belirtilen sorularımın, Ulaştırma ve Altyapı Bakanı Abdulkadir Uraloğlu tarafından Anayasa'nın 98'inci ve Türkiye Büyük Millet Meclisi İçtüzüğü'nün 96'ncı ve 99'uncu maddeleri uyarınca yazılı olarak cevaplandırılmasını saygılarımla arz ederim. 18.06.2026

**Av. Mahmut TANAL**  
**CHP Şanlıurfa Milletvekili**

Dijitalleşmenin hızla yayıldığı günümüzde, devletlerin bağımsızlığı yalnızca kara, hava ve deniz sınırlarının korunmasıyla değil; veri güvenliği, siber egemenlik ve dijital altyapılarının güvenliğiyle de doğrudan ilişkilidir.

Türkiye Büyük Millet Meclisi, Cumhurbaşkanlığı, bakanlıklar, yargı organları, güvenlik kurumları ve kritik kamu altyapıları; milyonlarca vatandaşa ait verilerin işlendiği, devlet sırlarının korunduğu ve kamu hizmetlerinin yürütüldüğü stratejik yapılardır. Bu nedenle söz konusu kurumlarda kullanılan bilgi teknolojileri altyapılarının güvenliği, doğrudan milli güvenlik meselesidir.

Cumhurbaşkanlığı tarafından yayımlanan Bilgi ve İletişim Güvenliği Genelgesi ile kamu kurumlarında yerli ve milli yazılımların kullanımının teşvik edilmesi, kritik verilerin yurt içinde tutulması ve yabancı teknoloji bağımlılığının azaltılması hedeflenmiştir. Buna rağmen kamu kurumlarının önemli bir bölümünde yabancı menşeli güvenlik duvarları (Firewall), web uygulama güvenlik sistemleri (WAF), saldırı tespit ve önleme sistemleri ile ağ güvenliği çözümlerinin kullanılmaya devam ettiği bilinmektedir.

Yabancı menşeli siber güvenlik ürünlerinin kullanılması; veri güvenliği, kişisel verilerin korunması, kamu verilerinin yabancı şirketlerin kontrolündeki sistemlerden geçmesi, dış müdahalelere açıklık ve dijital bağımsızlık bakımından çeşitli riskler doğurmaktadır.

Öte yandan yerli mühendisler tarafından geliştirilen çok sayıda siber güvenlik ürünü bulunmasına rağmen, kamu ihalelerinde uygulanan teknik şartnameler, uluslararası sertifikasyon zorunlulukları ve çeşitli bürokratik engeller nedeniyle yerli firmaların kamu pazarına erişiminde ciddi güçlükler yaşandığı yönünde iddialar bulunmaktadır.

Ayrıca milletvekillerinin, siyasi partilerin, kamu kurumlarının ve yerli girişimlerin internet sitelerinin yabancı menşeli filtreleme sistemleri tarafından "Yeni Alan Adı", "Sınıflandırılmamış Site", "Riskli İçerik" gibi kategoriler altında erişim kısıtlamalarına maruz kalabildiği görülmektedir. Bu durum bilgiye erişim hakkı, ifade özgürlüğü ve dijital egemenlik açısından ayrıca değerlendirilmesi gereken bir husustur.

Türkiye'nin dijital bağımsızlığının güçlendirilmesi, kamu verilerinin korunması, yerli yazılım sektörünün desteklenmesi ve kamu kaynaklarının etkin kullanılması amacıyla aşağıdaki soruların cevaplandırılması önem arz etmektedir.

Bu bağlamda;

1. Türkiye Büyük Millet Meclisi, Cumhurbaşkanlığı, bakanlıklar ve bağlı kamu kurumlarında aktif olarak kullanılan siber güvenlik ürünleri, güvenlik duvarları (Firewall), web uygulama güvenlik sistemleri (WAF), saldırı önleme sistemleri ve ağ güvenliği çözümlerinin kaç tanesi yerli ve milli imkanlarla geliştirilmiştir?

2. Kamu kurumlarında kullanılan siber güvenlik ürünlerinin marka ve menşe ülkelerine göre dağılımı nedir?
3. Son 5 yıl içerisinde kamu kurumlarının yabancı menşeli siber güvenlik ürünleri için ödediği lisans, abonelik, bakım ve destek bedellerinin yıllara göre toplam tutarı ne kadardır?
4. Kamu kurumlarında kullanılan yabancı menşeli güvenlik duvarlarının, trafik analizi, log yönetimi, telemetri verileri veya kullanıcı metadatalarını yurt dışındaki sunuculara aktarıp aktarmadığına ilişkin herhangi bir teknik inceleme, denetim veya bağımsız güvenlik testi yapılmış mıdır? Yapılmış ise bu incelemelerin sonuçları nelerdir?
5. TBMM'nin internet trafiği, ağ kayıtları ve sistem loglarının tamamı Türkiye sınırları içerisinde mi tutulmaktadır?
6. TBMM ve diğer kamu kurumlarında kullanılan güvenlik sistemlerinin kaynak kod incelemesi veya güvenlik denetimi yapılmakta mıdır?
7. Bilgi ve İletişim Güvenliği Genelgesi kapsamında kamu kurumlarında yerli yazılım kullanım oranının artırılması için yürütülen çalışmalar nelerdir?
8. Kamu ihalelerinde yerli siber güvenlik firmalarının katılımını zorlaştırdığı iddia edilen yabancı sertifikasyon ve lisans şartlarının kaldırılmasına veya kolaylaştırılmasına yönelik bir çalışma bulunmakta mıdır?
9. Son beş yılda kamu kurumlarının açtığı siber güvenlik ihalelerine kaç yerli firma katılmıştır? Kaç ihale yerli firmalar tarafından kazanılmıştır?
10. Milletvekillerinin resmi internet sitelerinin ve yerli kurumsal web sitelerinin yabancı filtreleme sistemleri tarafından erişim engeline uğramasının önlenmesi amacıyla BTK veya USOM bünyesinde milli bir kategorizasyon ve beyaz liste sistemi kurulması planlanmakta mıdır?
11. Türkiye'de geliştirilen yerli web uygulama güvenlik duvarları ve diğer siber güvenlik çözümlerinin TBMM ve kamu kurumlarında pilot uygulama olarak test edilmesine yönelik herhangi bir proje yürütülmekte midir?
12. Kamu kurumlarında kullanılan yabancı menşeli siber güvenlik ürünlerinin oluşturabileceği ulusal güvenlik risklerine ilişkin hazırlanmış herhangi bir risk analizi veya etki değerlendirme raporu bulunmakta mıdır?
13. Türkiye'nin dijital egemenliğini güçlendirmek ve kamu kurumlarında yerli siber güvenlik ürünlerinin kullanımını artırmak amacıyla Bakanlığınızın kısa, orta ve uzun vadeli stratejik planları nelerdir?
14. Kamu kurumlarında kullanılan siber güvenlik altyapılarında yerli ürün kullanım oranının artırılmasına yönelik belirlenmiş somut hedefler ve takvim mevcut mudur?