www.ddsgd.org

TBMM Plan ve Bütçe Komisyonu'nda Kabul Edilen

"Bazı Kanunlarda ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Teklifi (Esas No: 2/3764)" 19. Maddesi Hakkında

DEĞERLENDİRME NOTU

16 Temmuz 2026

Türkiye'de İnternet Kısıtlama Usulüne Yönelik Düzenleme Teklifinin Dijital Ekonomi Ve Uluslararası Uyum Perspektifinden Değerlendirilmesi

TANER ÇITAK

DİJİTAL DÖNÜŞÜM VE SİBER GÜVENLİK DERNEĞİ-DDSGD KURUCU BAŞKANI

1.GİRİŞ

Kamu ve özel sektörün gündeminde olan ve milli çözümlerle desteklenmesi yönünde stratejilerin izlendiği **"veri merkezleri"**nin etkisi çok boyutlu olarak ele alınması gereken bir alandır. Bu önemi dikkate alarak oluşturulan millileşme temelli stratejiler memnuniyet vericidir.

Ülkemiz, veri merkezlerine yönelik büyük bir potansiyeli barındırmaktadır. Veri bağımsızlığını korumak için geliştirilen ve geliştirilecek yazılım ve donanımlar, buna ilave olarak küresel firmaların veri merkezi yatırımlarıyla büyük bir ekosistem inşa edilebilir.

Veri merkezlerinde Türkiye pazar büyüklüğünün 2031'e kadar 1,79 milyar dolara çıkacak olması, nitelikli işgücü ve gençlerimiz için yeni ve büyük bir istihdam ekosistemi yaratacaktır. Türkiye, bu büyüklüğün çok daha ötesinde bir potansiyele sahiptir. Yapay zeka uygulamalarının katlanarak etkinliğinin arttığı bir ortamda, veri merkezlerinin sadece Türkiye değil, dünyada da tahminlerin ötesinde bir büyümesi şaşırtıcı olmayacaktır.

Önemle vurgulanması gereken husus, veri merkezleri ve siber güvenlik ülkelerin kendi veri merkezlerine sahip olmak basit birer ticari-teknoloji altyapıdan çok ödeye anlamlar taşımaktadır. Hem milli veri merkezleri, hem de dış yatırımların gelişmesi, bu alandaki hukuki düzenlemelerin özgürlük-güvenlik dengesinin çok hassas şekilde ayarlanmasını gerekli kılmaktadır.

Bu çereçevede ele aldığımız TBMM Plan ve Bütçe Komisyonu'nda kabul edilen Bazı Kanunlarda ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Teklifi (Esas No: 2/3764) 19. Maddesi'nde öngörülen düzenlemenin bazı ciddi riskler barındırdığını değerlendiriyoruz.

Kabul edilen Teklifin 19'uncu maddesi; internet içeriklerine ilişkin kısıtlama yetkilerinin Bilgi Teknolojileri ve İletişim Kurumu'ndan (BTK) Siber Güvenlik Başkanlığı'na devrini, Başkanlığın resen veya güvenlik ve istihbarat kurumlarının talebi üzerine karar alabilmesini, kararların servis sağlayıcılarca 2 saat içinde uygulanmasını ve 48 saat içinde sulh ceza hâkimliği onayına sunulmasını öngörmektedir.

Bu değerlendirme notu, düzenlemeyi öncelikle ekonomik ve uluslararası uyum perspektifinden ele almaktadır. Temel tespit şudur: Düzenleme mevcut haliyle, güvenlik hedeflerinin ötesine taşan bir öngörülemezlik alanı yaratarak ülkeyi küresel dijital ekonomiden izole etme risklerini barındırmaktadır. Yabancı yatırım, veri merkezi ve bulut altyapısı kararlarının hukuki öngörülebilirliğe son derece duyarlı olduğu bir dönemde, süreç güvencelerinin güçlendirilmesi hem güvenlik hedeflerine hem de dijital ekonomi hedeflerine birlikte hizmet edecektir.

Değerlendirme; düzenlemenin öngördüğü yapısal değişiklikleri, izolasyon risklerini, anayasal çerçeveyi ve ABD ile AB modellerinin sadeleştirilmiş özetlerini içermekte; sonuç bölümünde yapıcı politika önerileri sunmaktadır.

2. Düzenlemenin Öngördüğü Yapısal Değişiklikler

Yetki devri: İnternet içeriklerine ilişkin kısıtlama yetkileri, düzenleyici bir kurum olan BTK'den, doğrudan yürütmeye bağlı çalışan Siber Güvenlik Başkanlığı'na geçmektedir. Bu tercih, konuyu iletişim ve altyapı düzleminden ulusal güvenlik düzlemine taşımaktadır.

Resen yetki ve "gecikmesinde sakıncalı hal": Başkanlık, resen veya güvenlik ve istihbarat kurumlarının talebi üzerine harekete geçebilecektir. "Gecikmesinde sakıncalı hal" kavramının kanunda somut kriterlerle tanımlanmaması, uygulamada geniş bir takdir alanı doğurmaktadır.

Süreç sıralaması: Kararlar önce uygulanmakta (2 saat), yargısal değerlendirme sonradan (48 saat içinde) devreye girmektedir. Dijital iletişimin hızı dikkate alındığında, bu sıralama yargısal denetimin fiilî etkisini sınırlandırabilmektedir.

Alan adı (domain) yetkileri: İnternet alan adlarına yönelik strateji, politika ve düzenleme yetkilerinin Başkanlığa verilmesi, teknik bir güvenlik kurumuna aynı zamanda yayın ekosistemini etkileyebilecek araçlar kazandırmakta; uymayan servis sağlayıcılar ve veri merkezleri için idari para cezaları öngörülmektedir.

3. Temel Risk Alanı: Küresel Dijital Ekonomiden İzolasyon

Düzenlemenin en önemli ve çoğu zaman gözden kaçan boyutu ekonomiktir. Uluslararası dijital ekonomiye entegrasyon; sermaye, veri ve hizmet akışlarının kesintisizliğine ve hukuki öngörülebilirliğe dayanır. Aşağıdaki risk başlıkları bu çerçevede öne çıkmaktadır:

- **Yatırım ortamı ve veri merkezi kararları:** Küresel bulut sağlayıcıları ve veri merkezi yatırımcıları, lokasyon seçiminde düzenleyici öngörülebilirliği başlıca kriter olarak değerlendirmektedir. İçerik veya alan adlarının kısa süreler içinde idari kararla erişime kapatılabildiği bir çerçeve, Türkiye'nin bölgesel veri merkezi üssü olma hedefiyle gerilim oluşturabilir.
- **Yerli girişim ekosistemi:** Alan adları ve barındırma altyapısı üzerindeki idari yükümlülükler ve yaptırım riski; yerli teknoloji girişimlerinin, e-ticaret platformlarının ve yazılım ihracatçılarının maliyetlerini artırabilir, uluslararası müşteri ve yatırımcı nezdinde rekabet gücünü zayıflatabilir.
- **AB dijital tek pazarıyla uyum:** Avrupa Birliği, Dijital Hizmetler Yasası (DSA) ile şeffaflık ve süreç güvencelerini dijital ticaretin ön koşulu haline getirmiştir. Türkiye'nin çerçevesinin bu standartlardan uzaklaşması; veri akışları, dijital hizmet ihracatı ve olası yeterlilik/uyum değerlendirmeleri bakımından ilave engeller doğurabilir.
- **Kontrol dışı mecralara kayış:** Erişilebilir ve kayıtlı mecraların daralması bilgi akışını durdurmamakta; kullanıcıları VPN'lere ve denetimi çok daha güç, uçtan uca şifreli kanallara yönlendirmektedir. Bu durum, düzenlemenin kamu düzenini koruma amacını zayıflatabilecek bir yan etki üretmektedir.
- **İtibar ve endeks etkileri:** Uluslararası dijital özgürlük ve iş yapma kolaylığı endekslerindeki olası gerilemeler, doğrudan yabancı yatırım kararlarında ve teknoloji ortaklıklarında referans olarak kullanılmakta; izolasyon etkisini kendi kendini besleyen bir döngüye dönüştürebilmektedir.

Bu risklerin ortak paydası şudur: Sorun, güvenlik amacının kendisi değil; amacı gerçekleştirmek için seçilen araçların, dijital ekonominin işleyişi için vazgeçilmez olan **öngörülebilirlik ve süreç güvencesi** beklentileriyle henüz tam uyumlu olmamasıdır.

4. Anayasal Çerçeve Açısından Değerlendirme

Düzenlemenin, Anayasa'nın 22'nci maddesindeki haberleşme hürriyeti ve 13'üncü maddesindeki sınırlama rejimi ile uyumunun güçlendirilebileceği başlıca noktalar şunlardır:

- **Hâkim kararı esası (Md. 22/2):** Anayasa, haberleşme hürriyetine müdahalede hâkim kararını asıl, idari merci emrini dar yorumlanması gereken bir istisna olarak kurgular. Yetkinin operasyonel bir güvenlik yapısında toplanması, bu istisnanın asıl kurala dönüşmesi riskini taşımaktadır.
- **Hukuki belirlilik:** "Gecikmesinde sakıncalı hal" ibaresinin somut kriterlere bağlanmaması, vatandaşların ve işletmelerin hangi fiilin hangi sonucu doğuracağını öngörmesini güçleştirmekte; belirlilik ilkesi yönünden tartışma alanı açmaktadır.
- **Ölçülülük (Md. 13):** İki saatlik uygulama zorunluluğu ve alan adı düzeyindeki müdahale imkânı, amaçla araç arasındaki orantılılık testinin titizlikle işletilmesini gerektirmekte; hakkın özüne dokunma yasağı bakımından hassasiyet taşımaktadır.
- **Etkili başvuru (Md. 36):** Yargısal değerlendirmenin müdahale gerçekleştikten sonra devreye girmesi, telafisi güç zararlar bakımından hak arama hürriyetinin etkinliğini azaltabilmektedir. Onay süreçlerinin gerekçeli ve esaslı bir inceleme olarak tasarlanması bu riski azaltacaktır.

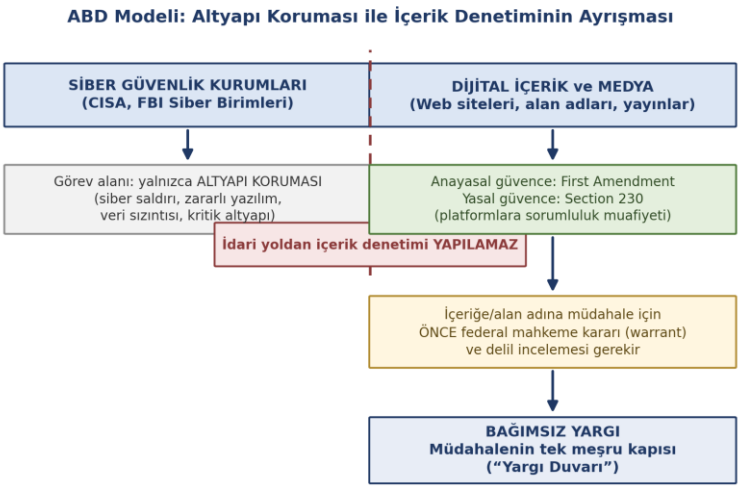
5. Uluslararası Uygulama Modelleri

Aşağıdaki iki model, demokratik hukuk sistemlerinde siber güvenlik ile içerik yönetiminin nasıl ayrıştırıldığını özetlemektedir. Her iki modelin ortak noktası; siber güvenlik kurumlarının görev alanının **altyapı koruması** ile sınırlı tutulması ve içerik müdahalelerinin şeffaf, gerekçeli ve yargı güvenceli süreçlere bağlanmasıdır.

5.1. ABD Modeli

ABD'de ifade özgürlüğü, Anayasa'nın Birinci Değişikliği (First Amendment) ile güçlü biçimde korunur; devletin içerik temelli kısıtlama yapması ancak çok dar istisnalarla mümkündür. Section 230, platformları kullanıcı içeriklerinden doğan hukuki sorumluluktan büyük ölçüde muaf tutar; içerik moderasyonu esasen platformların kendi kurallarına bırakılmıştır.

Cybersecurity and Infrastructure Security Agency Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) ve FBI siber birimleri gibi kurumların görevi münhasıran altyapı korumasıdır (siber saldırı, zararlı yazılım, kritik altyapı güvenliği); içerik veya medya denetimi yetkileri yoktur. Bir alan adına el konulması ya da bir sitenin kapatılması, kural olarak ancak mahkeme kararı (warrant) ve delil incelemesiyle mümkündür. Bu yapı literatürde "Yargı Duvarı" olarak anılır.

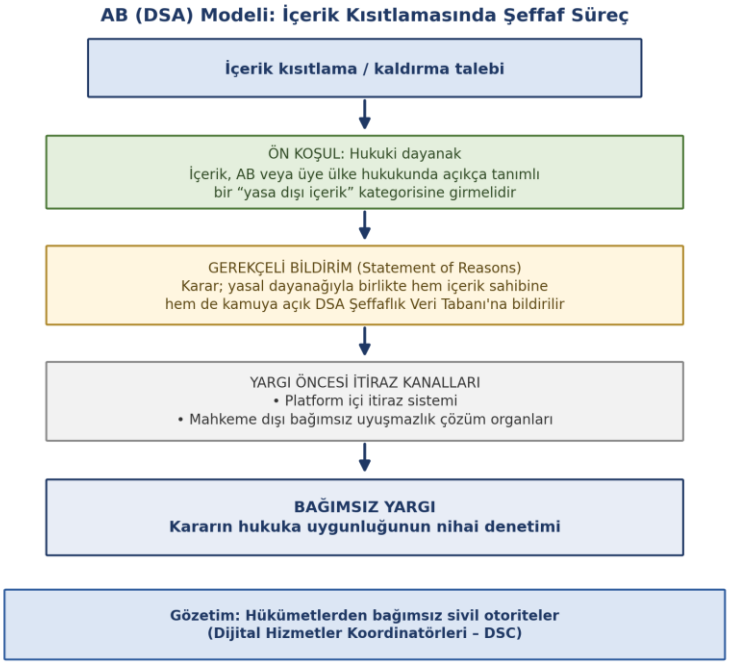


Şekil 1 — ABD modelinde altyapı koruması ile içerik denetiminin kurumsal ayrışması

5.2. AB (DSA) Modeli

Avrupa Birliği'nde dijital alanın gözetimi, Dijital Hizmetler Yasası (DSA) kapsamında güvenlik bürokrasisine değil, hükümetlerden bağımsız sivil otoriteler olan Dijital Hizmetler Koordinatörlerine (DSC) verilmiştir. Bir içeriğe müdahale edilebilmesi için içeriğin AB veya üye ülke hukukunda açıkça tanımlanmış bir "yasa dışı içerik" kategorisine girmesi şarttır; "dezenformasyon" veya siyasi eleştiri gibi soyut gerekçeler tek başına yeterli değildir.

Her kısıtlama kararı, yasal dayanağını içeren bir Gerekçeli Bildirim (Statement of Reasons) ile hem içerik sahibine bildirilmek hem de kamuya açık DSA Şeffaflık Veri Tabanı'na işlenmek zorundadır. Kullanıcılar, mahkeme sürecini beklemeden platform içi itiraz sistemlerine ve mahkeme dışı bağımsız uyuşmazlık çözüm organlarına başvurabilir; nihai denetim bağımsız yargıya aittir.



Şekil 2 — AB (DSA) modelinde içerik kısıtlamasının şeffaf süreç akışı

5.3. Karşılaştırma Özeti

Kriter	ABD / AB Modelleri	Teklifin Mevcut Hali
Yetkili kurum	Bağımsız sivil otoriteler ve mahkemeler	Yürütmeye bağlı Siber Güvenlik Başkanlığı
Kısıtlama gerekçesi	Hukukta açıkça tanımlı yasa dışı içerik kategorileri	"Gecikmesinde sakıncalı hal" gibi genel kavramlar
Süreç sıralaması	Önce hukuki değerlendirme ve güvenceler, sonra uygulama	Önce uygulama (2 saat), sonra yargısal onay (48 saat)
Şeffaflık	Gerekçeli bildirim ve kamuya açık kayıt (DSA)	Karşılaştırılabilir bir şeffaflık mekanizması öngörülmemiştir
Siber güvenliğin kapsamı	Altyapı ve şebeke koruması	İçerik ve alan adı yönetimini de kapsayacak şekilde genişlemektedir

6. Sonuç ve Politika Önerileri

Siber tehditlerin arttığı bir dönemde kurumsal kapasitenin güçlendirilmesi meşru ve gerekli bir hedeftir. Değerlendirmemiz, bu hedefin kendisine değil, hedefe ulaşmak için seçilen usul tasarımına ilişkindir. Düzenleme mevcut haliyle; öngörülebilirliği zayıflatan geniş takdir alanları, önce uygulama sonra denetim sıralaması ve alan adı düzeyine uzanan yetkiler nedeniyle, **ülkeyi küresel dijital ekonomiden izole etme risklerini barındırmaktadır.** Bu riskin yönetilebilir olduğu ve aşağıdaki uyarlamalarla hem güvenlik hem de ekonomi hedeflerinin birlikte gerçekleştirilebileceği değerlendirilmektedir:

- **Kavramların netleştirilmesi:** "Gecikmesinde sakıncalı hal" kavramının, kanunda sayılan somut ve dar suç kategorilerine bağlanması.
- **Yargısal güvencenin öne alınması:** Gerçek aciliyet halleri dışında hâkim kararının müdahaleden önce alınmasının esas kılınması; sonradan onay usulünün gerekçeli ve esaslı incelemeye tabi tutulması.
- **Görev ayrışması:** Siber Güvenlik Başkanlığı'nın görev tanımının altyapı ve şebeke korumasına odaklanması; içerik ve alan adı süreçlerinde sivil ve bağımsız denetim mekanizmalarının korunması.
- **Şeffaflık mekanizması:** DSA'daki gerekçeli bildirim uygulamasına benzer şekilde, kısıtlama kararlarının gerekçeleriyle birlikte kayıt altına alındığı ve düzenli raporlandığı bir şeffaflık çerçevesi kurulması.
- **Etki analizi:** Düzenlemenin veri merkezi yatırımları, girişim ekosistemi ve AB dijital mükteseatıyla uyum üzerindeki etkilerine ilişkin düzenli ekonomik etki analizlerinin yapılması.

Bu uyarlamalar, güvenlik kapasitesinden ödün vermeksizin; yatırımcı güvenini, uluslararası uyumu ve anayasal güvenceleri güçlendirecek, Türkiye'nin küresel dijital ekonomideki konumunu koruyacaktır.