Dijital Dönüşüm ve Siber Güvenlik Derneği Başkanı Taner Çıtak TBMM Plan Bütçe Komisyonu'nda kabul edilen internet erişimi yasağı düzenlemesini değerlendirdi:

Türkiye veri merkezlerinde genç istihdamı başta büyük potansiyele sahip

Aşırı kontrol, kontrolsüz alanlara kayışa neden olabilir

Yerli veri merkezi yatırımcıları olumsuz etkilenebilir

Özgürlük-güvenlik dengesiyle düzenleme mümkün

ANKARA - Dijital Dönüşüm ve Siber Güvenlik Derneği (DDSGD) Başkanı Taner Çıtak, Türkiye'nin veri merkezleri sektöründe başta gençlerin istihdamı olmak üzere büyük bir potansiyele sahip olduğunu, bu potansiyelin harekete geçirilmesi için özgürlük-güvenlik dengesinin hassas biçimde sağlanması gerektiğini belirtti.

TBMM Plan ve Bütçe Komisyonu'nda kabul edilen internet erişiminin kısıtlanma usulü düzenlemesi hakkında Taner Çıtak tarafından hazırlanan değerlendirme notu DDSGD tarafından yayınlandı. Değerlendirmede, kısıtlayıcı yönde aşırı düzenlemelerin, hem yerli, hem de yabancı yatırımcıyı olumsuz etkileyeceği, hem de kontrol arayışlarına karşılık kontrol dışındaki alanlara yönelmeye neden olabileceği uyarısında bulunuldu.

Değerlendirme notunda, kamunun yanında özel sektörün de veri merkezleri, siber güvenlik başta olmak üzere dijital ekonomideki farkındalığı bulunduğu ve bu alanda izlenen milli çözümler geliştirme yanında yabancı doğrudan yatırım çekme girişimlerinin de olumlu olduğu vurgulandı. Buna karşılık, TBMM'de kabul edilen düzenlemenin bu anlayış ve yaklaşımı karşılamadığı vurgulandı.

-Risk alanları: Temel risk, çoğu zaman gözden kaçan "ekonomik boyut"

Taner Çıtak tarafından hazırlanan değerlendirme notunda, bu tür düzenlemelerde ekonomik boyutun gözden kaçabildiğini vurgulayarak, riskin küresel dijital ekonomiden izolasyona kadar varabileceğine dikkat çekildi.

"Düzenlemenin en önemli ve çoğu zaman gözden kaçan boyutu ekonomiktir. Uluslararası dijital ekonomiye entegrasyon; sermaye, veri ve hizmet akışlarının kesintisizliğine ve hukuki öngörülebilirliğe dayanır" denilen notta, "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" ifadesine yer verildi. Değerlendirmede, yerli ve yabancı yatırım kararlarından AB'nin dijital tek pazarına uyumun bozulmasına kadar risk alanları şöyle sıralandı:

- 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.

-Nasıl bir yol izlenmeli?

Değerlendirme notunda, yapılması gereken iyileştirmeler ve bu alandaki politika önerilerine de yer verildi. Taner Çıtak'ın değerlendirmesinde, siber tehditlerin arttığı bir ortamda kurumsal kapasitenin güçlendirilmesinin gerekli olduğuna işaret edilirken, bu güçlendirme için seçilen araç ve usulün hassas olması gerektiğine vurgu yapıldı.

Bu yaklaşımla, düzenlemenin mevcut halinin öngörülebilirliği zayıflatan, idareye geniş takdir hakkı tanıdığı, önce uygulama, sonra denetim sıralamasının ülkeyi küresel dijital ekonomiden özole etme riski barındırdığına dikkat çekildi. Güvenlik ve ekonominin birlikte gerçekleşebilmesi için yapılması gereken iyileştirmeler şöyle sıralandı:

- 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 müktesebatıyla uyum üzerindeki etkilerine ilişkin düzenli ekonomik etki analizlerinin yapılması.

Bilgi notunda, yapılan düzenlemeler ekonomik etki yanında, Anayasal çerçeve açısından değerlendirildi ve ABD ile Avrupa uygulamaları incelendi. Bu kapsamda, Anayasa açısından haberleşme hürriyeti ile hakim kararı esasına rağmen yetkinin idaredeki operasyonel bir güvenlik birimine verilmesinin, istisnanın kural haline gelmesi riski doğurduğuna dikkat çekildi. Ayrıca,

“gecikmesi sakıncalı hal” kavramının hukuki somut kriterlere bağlanmasının yaratacağı belirsizliğin sorun noktası olduğu, iki saatte uygulama zorunluluğu, alan adı düzeyinde müdahale imkanının amaç ile araç arasında orantısızlık yarattığı vurgulandı. Yargısal değerlendirmenin müdahaleden sonraya bırakılmasının da telafisi güç zararlar bakımından hak arama hürriyetinin etkinliğini azaltacağına dikkat çekildi.

Ülke uygulamaları ve Kanun Teklifi düzenlemesi 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