

BASIN AÇIKLAMASI

TARİH: 16 Ocak 2025

İfade Özgürlüğü Derneği

Siber Güvenlik Kanunu Teklifi: Tehlikenin Farkında Mısınız?

İfade Özgürlüğü Derneği, Türkiye Büyük Millet Meclisi'nde sunulan **Siber Güvenlik Kanunu Teklifine** ilişkin görüş ve endişelerini **kamuoyuyla paylaşarak**, ifade özgürlüğü, kişisel verilerin korunması ve özel hayatın gizliliği gibi temel insan haklarını tehdit eden ciddi risklere dikkat çekmeyi amaçlamaktadır. Siber güvenliğin güçlendirilmesi hedefiyle sunulan bu teklif, yalnızca “**Orwellian**” bir yaklaşımı çağrıştırmakla kalmayıp, bireylerin hak ve özgürlüklerini doğrudan kısıtlayabilecek düzenlemeler içermektedir. Tasarı, 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. Temel hak ve özgürlüklerin korunması adına, teklifin mevcut haliyle kabul edilmesi mümkün değildir; derinlemesine gözden geçirilmesi ya da tamamen geri çekilmesi zorunludur.

Yasalık İlkesinin Ağır İhlali

Kurumsal Belirsizlik

Siber Güvenlik Kanunu Teklifi, kapsamı ve kurduğu Siber Güvenlik Başkanlığı'nın yetkileri açısından ciddi belirsizlikler içermektedir. Yasa teklifi, Türk hukukunda daha önce tanımlanmamış olan “kritik altyapı” ve “kritik kamu hizmeti” gibi soyut kavramları ilk kez kapsamına almaktadır. Ancak, Yasada bu kavramların içeriği açık bir şekilde belirtilmemiş, 5. madde ile bu belirleme yetkisi doğrudan Başkanlığa bırakılmıştır. Bu durum, yasama yetkisinin idareye devri anlamına gelmekte ve Başkanlığın keyfi olarak özerk olması gereken üniversiteler, bağımsız idari otoriteler gibi kurumları kritik altyapı ilan etmesinin önünü açmaktadır. Böyle bir tanımlama, özerk olması gereken kurumların tüm faaliyetlerini Başkanlığın denetimi altına alabilir ve işbirliği yapmayanlara 16. madde uyarınca ağır yaptırımlar uygulanmasına neden olabilir.

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)

Ancak Siber Güvenlik Kanun Teklifi bu ilkeyi de tümüyle göz ardı etmektedir. Örneğin, yasa metninde adı geçen “SOME” (Siber Olaylara Müdahale Ekibi) isimli birimle ilgili herhangi bir açıklama bulunmamaktadır. 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,

Yasa'nın 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 özgürlükleri ciddi bir şekilde tehdit etmektedir.

Suç ve Cezaların Belirsizliği

Siber Güvenlik Kanunu Teklifindeki belirsizlik sadece kurumsal yapı ve görevler açısından söz konusu değildir. Yasanın yeni ihdas ettiği 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 keyfi 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 ölçsüzlüğü, hukuk devleti ilkesine aykırılık teşkil etmekte ve bireylerin temel haklarını ağır şekilde ihlal etme riski taşımaktadır.

Başkanlığın Görevlerinin Belirsizliği

Özel Hayatın Gizliliği ve Kişisel Veriler Tehlike Altında

Yakın tarihte Cumhurbaşkanlığı kararnamesiyle kurulan ve yasa teklifiyle geniş yetkilerle donatılması planlanan **Siber Güvenlik Başkanlığı**, özel hayatın gizliliği ve kişisel verilerin korunması açısından ciddi bir tehdit oluşturmaktadır (**Resmi Gazete, 08.01.2025, Sayı: 32776**). Her ne kadar yasa teklifinin amacı, siber güvenliği güçlendirmek ve kritik altyapıyı korumak olarak ifade edilse de, 6. maddede tanımlanan yetkiler, **yasal güvenceden yoksun**, keyfi uygulamalara yol açabilecek ve denetlenemeyen bir sistem öngörülmektedir.

Hakim Onayı Olmaksızın Her Türlü Bilgiye Erişim Yetkisi: Kişisel Mahremiyet Tehlikede

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.

Kişisel Verilere Keyfi Erişim: Denetim Dışı Bir Güç

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.

Anayasa Mahkemesi'nin İçtihatlarına Aykırı

Yasa teklifinin 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 verilerin korunmasını isteme hakkını sınırlamaya yönelik kanuni bir düzenlemenin **şeklen var olması yeterli olmayıp yasal kuralların keyfilğe izin vermeyecek şekilde belirli ve öngörülebilir düzenlemeler niteliğinde olması gerekir** (Anayasa Mahkemesi, E.: 2018/91 K.: 2020/10, 19.02.2020, § 95).

Anayasa Mahkemesi, 5651 Sayılı Kanununda Yer Alan Benzer Yetkileri İptal Etmiştir

Anayasa Mahkemesi, öncelikle “*Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden temin edilir ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verilir*” hükmünü iptal etmiş (AYM, E. 2014/149, K. 2014/151, 02.10.2014) arkasından da “*Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle*” ilgili hükmü de Anayasa'ya aykırı bulmuş ve iptal etmiştir (AYM, E. 2014/87, K. 2015/112, 08.12.2015). 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 edilmiştir. Mahkeme, trafik bilgisi adı altında temin edilecek olan bilgilerin birçok temel hakla doğrudan ilgili olup bu bilgilerin BTK tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olmasını temel hak ve özgürlüklerin korunması bakımından sorunlu bulmuş ve keyfiyete izin verdiğini belirtmiştir.

Hak Arama Hürriyetine Müdahale

Benzer bir durum şimdi de **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 görecekt kişilerin Başkanlığın bilinmeyen ve **hakim onayı şartı aranmayan kararlarına** karşı hukuki yollara başvurusu, 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.

Siber Güvenlik Başkanlığı ve Bağımsız Demokratik Denetim Gerekliliği

Teklif, Başkanlığa geniş yetkiler tanınmasına rağmen bu yetkilerin kullanımıyla ilgili herhangi bir bağımsız denetim mekanizması öngörmemektedir. Başkanlığın keyfi işlemleriyle zarar görecektir 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 fakat imha edilip, edilmeyeceği hususunda herhangi bir yasal güvence sunulmamış, 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.

Bir başka deyişle, Yasada herhangi bir **bağımsız denetim mekanizması** öngörülmemiş, kişisel verilerin korunmasına ilişkin genel ifadeler **belirsiz ve öngörülemez** bir çerçevede sunulmuştur. Dolayısıyla, denetim mekanizmalarının tamamen eksikliği, bu tür geniş yetkilerin keyfi kullanımına kapı aralamaktadır.

İfade Özgürlüğüne Tehdit: Belirsiz, Keyfi ve Baskıcı Düzenlemeler

Siber Güvenlik Kanunu Teklifi, yalnızca kişisel verilerin korunması ve özel hayatın gizliliği konularında değil, aynı zamanda **ifade özgürlüğü** üzerinde ciddi kısıtlamalar yaratabilecek hükümler içermektedir. Yukarıda açıklandığı üzere yasadaki hükümler hangi eylemlerin suç olarak düzenlendiğini açık bir şekilde tarif etmediği için öncelikle yasallık ilkesine aykırıdır. Ancak bunun yanında ilgili kuralların ayrıca Anayasa’da korunan temel hak ve özgürlükleri ciddi anlamda tehdit etmektedir. Teklifin, özellikle **16. maddesinin 5. fıkrası**, ifade özgürlüğüne yönelik yeni bir tehdit unsuru oluşturmakta ve belirsizliklerle dolu, keyfiyete açık bir düzenleme sunmaktadır.

Algı Üzerinden Suçlama: Keyfi ve Belirsiz Tanımlamalar

Teklif edilen Yasanın 16. maddenin 5. fıkrası, “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” hükmünü içermektedir. Ancak, “**algı oluşturmak**” gibi soyut ve yoruma açık bir fiilin tanımlanmamış olması, yasanın uygulanmasında keyfiyete zemin hazırlamaktadır. Söz konusu hüküm, Milli Savunma Komisyonu’nda şu şekilde değiştirilmiştir: “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 veya bu içerikleri yayanlara 2 yıldan 5 yıla kadar hapis cezası verilecek” şeklinde değiştirilmiştir. Ancak bu değişiklik, **yasa metninin belirsizliklerini gidermek yerine**, daha önce büyük eleştirilere hedef olan Türk Ceza Kanunu’nun **217/A maddesindeki** “Halkı yanıltıcı bilgiyi alenen yayma suçu” ve yasalasmayan “etki ajanlığı” suçlarıyla benzer sorunları yeniden gündeme taşımaktadır.

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 nedenle, bu tür düzenlemelerin, “**hassas**” olarak nitelendirilen konularda eleştirel görüşlerin susturulması için bir araç haline dönüşme riski son derece yüksektir. 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.

Sonuç: Temel Hakların Korunması İçin Acil Gözden Geçirme Zorunluluğu

Siber Güvenlik Kanunu Teklifi, siber güvenliğin sağlanmasını hedefleyen bir düzenleme olarak temel hak ve özgürlüklerin korunmasıyla uyumlu olmak zorundadır. Ancak, teklifin mevcut hali, ifade özgürlüğü, kişisel verilerin korunması ve özel hayatın gizliliği gibi demokratik toplumun temel değerlerini ciddi şekilde tehlikeye atmaktadır. Yasa teklifinin içerdiği **belirsiz ve keyfi düzenlemeler**, yasal güvencelerden yoksun yetkiler ve bağımsız denetim mekanizmalarının eksikliği, bireylerin haklarını derinden zedeleyebilecek niteliktedir.

Bu bağlamda, İfade Özgürlüğü Derneği olarak aşağıdaki hususları vurguluyoruz:

1. **Yasa teklifi geri çekilmeli ve kapsamlı bir şekilde yeniden ele alınmalıdır.** Düzenlemeler, ulusal ve uluslararası hukuka uygun hale getirilmelidir.
2. **Kurumlar, suçlar ve görevler belirsizlikten arındırılmalıdır.** Yasanın kapsamına giren her türlü yetki ve tanım, Anayasa'nın öngördüğü şekilde öngörülebilir, belirli ve keyfiyete yer bırakmayacak bir biçimde düzenlenmelidir.
3. **Temel hak ve özgürlükleri sınırlandıran hükümlerde güçlü güvenceler sağlanmalıdır.** Özellikle ifade özgürlüğü ve özel hayatın korunması hakkı başta olmak üzere, temel hakları sınırlandıran hükümlerde hakim onayı şartı, bağımsız denetim mekanizmaları ve kişisel verilerin korunmasına yönelik güvenceler açık ve net bir şekilde ifade edilmelidir.
4. Siber güvenliğin güçlendirilmesi adına atılacak adımlar, **ifade özgürlüğünü** ve diğer **temel hakları ihlal etmeyecek şekilde** düzenlenmelidir.

Sonuç olarak, bu teklifin mevcut haliyle yasalaşması, demokratik toplum düzenine ve temel insan haklarına ciddi bir tehdit oluşturacaktır.

Kamuoyuna saygılarımızla duyurulur.

İfade Özgürlüğü Derneği