7545 SAYILI SİBER GÜVENLİK KANUNU VE İLETİŞİMİN DENETLENMESİ YETKİSİNİN DEVRİ

Kritik Altyapı Korumasından Erişim Yönetimine: 7590 Sayılı Kanunla Genişleyen Yetkiler, Yargısal Denetim Sorunu ve Sansür Riski

Türkiye's Cybersecurity Act No. 7545 and the Transfer of Communications Interception Powers: From Critical Infrastructure Protection to Access Control — Expanded Competences under Law No. 7590, Judicial Oversight and the Risk of Censorship

Derleme Makale / Review Article

Dr. Burak Olgun
burakolgun@solutionhome.net
Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Siber güvenlik hukuku • iletişimin denetlenmesi • erişim engelleme • yargısal denetim • ifade özgürlüğü

ÖZET

19 Mart 2025 tarihli ve 32846 sayılı Resmî Gazete'de yayımlanan 7545 sayılı Siber Güvenlik Kanunu, Türkiye'de siber güvenliği ilk kez müstakil bir kanunla düzenlemiş ve 177 sayılı Cumhurbaşkanlığı Kararnamesiyle kurulan Siber Güvenlik Başkanlığı'na kapsamlı görev ve yetkiler tanımıştır. 31 Temmuz 2026 tarihli ve 33326 sayılı Resmî Gazete'de yayımlanan 7590 sayılı Kanun ise bu yapıya ikinci bir katman eklemiş; internet alan adı yönetimi, internet altyapısı ve iletişimin tespiti ile analizi işlevlerini Bilgi Teknolojileri ve İletişim Kurumu'ndan Başkanlığa aktarmış ve Başkanlığa yargı kararını beklemeksizin acil tedbir belirleme yetkisi tanımıştır. Bu çalışma, söz konusu iki düzenlemeyi teknik ve hukuki boyutlarıyla incelemektedir. Çalışmada önce siber dayanıklılık, adli iletişimin denetlenmesi ve önleyici erişim yönetimi rejimlerinin birbirinden farklı hukuki temelleri ortaya konulmakta; ardından bu üç rejimin tek bir idari birimde toplanmasının doğurduğu sorunlar tartışılmaktadır. Kanun'un 8. maddesindeki arama ve el koyma yetkisi ile 16. maddesindeki ceza hükümleri -- özellikle veri sızıntısı iddiasına ilişkin fıkra -- belirlilik ilkesi ve caydırıcı etki bakımından değerlendirilmekte; acil tedbir mekanizmasının iki saatlik uygulama ve yirmi dört saatlik sunum süreleri, Avrupa İnsan Hakları Mahkemesi'nin gizli gözetim içtihadında geliştirdiği asgari güvence ölçütleriyle karşılaştırılmaktadır. Çalışma, düzenlemenin siber güvenlik gerekçesinin meşru olduğunu, ancak yetki genişliği ile yargısal denetimin sonraya bırakılmasının amaç kayması ve sansür aracı olarak kullanılma riskini yapısal biçimde artırdığını; bu riskin ancak süre sınırı, bildirim yükümlülüğü, bağımsız denetim ve şeffaflık raporlaması gibi somut güvencelerle dengelenebileceğini savunmaktadır.

Anahtar Kelimeler: *siber güvenlik hukuku, 7545 sayılı Kanun, 7590 sayılı Kanun, Siber Güvenlik Başkanlığı, iletişimin tespiti ve analizi, erişim engelleme, acil tedbir, yargısal denetim, sulh ceza hâkimliği, ifade özgürlüğü, sansür, amaç kayması, kritik altyapı, AİHM, orantılılık*

ABSTRACT

Cybersecurity Act No. 7545, published in Official Gazette No. 32846 of 19 March 2025, regulated cybersecurity through a dedicated statute for the first time in Türkiye and conferred extensive powers upon the Cybersecurity Directorate established by Presidential Decree No. 177. Law No. 7590, published in Official Gazette No. 33326 of 31 July 2026, added a second layer to this structure by transferring internet domain name management, internet infrastructure administration and

burakolgun.com

communications detection and analysis functions from the Information and Communication Technologies Authority to the Directorate, and by empowering the Directorate to impose urgent measures without awaiting a judicial decision. This study examines both instruments in their technical and legal dimensions. It first distinguishes the separate legal bases of cyber resilience, criminal interception and preventive access control regimes, then discusses the problems arising from consolidating all three within a single administrative body. The search and seizure power under Article 8 and the criminal provisions under Article 16 -- particularly the paragraph concerning allegations of data breaches -- are assessed in terms of legal certainty and chilling effect, while the two-hour implementation and twenty-four-hour submission periods of the urgent measure mechanism are compared against the minimum safeguards developed in the European Court of Human Rights case law on secret surveillance. The study argues that although the cybersecurity rationale is legitimate, the breadth of powers combined with deferred judicial review structurally increases the risk of function creep and use as an instrument of censorship, and that this risk can only be offset by concrete safeguards such as time limits, notification duties, independent oversight and transparency reporting.

Keywords: *cybersecurity law, Law No. 7545, Law No. 7590, Cybersecurity Directorate, communications interception, access blocking, urgent measures, judicial review, criminal judgeship of peace, freedom of expression, censorship, function creep, critical infrastructure, ECtHR, proportionality*

burakolgun.com

1. Giriş

Devletlerin siber uzaydaki savunma kapasitesini güçlendirme çabası, son on yılda dünyanın hemen her ülkesinde yeni kurumsal yapılar ve yeni yetkiler doğurmuştur. Kritik altyapıların hedef alındığı saldırıların can kaybına ve büyük ekonomik zarara yol açabilecek düzeye ulaşması, bu alandaki düzenleme ihtiyacını tartışmasız hâle getirmiştir. Ne var ki siber güvenlik yetkileri, doğası gereği ağ trafiğine, veri akışına ve iletişim altyapısına erişim gerektirdiğinden; aynı teknik kapasite, kullanıldığı amaca göre bir savunma aracı da bir gözetim aracı da olabilmektedir. Bu ikili nitelik, siber güvenlik hukukunun temel gerilimini oluşturur.

Türkiye'de bu gerilim, iki ayrı düzenleme dalgasıyla somutlaşmıştır. Birinci dalga, 19 Mart 2025 tarihli ve 32846 sayılı Resmî Gazete'de yayımlanan **7545 sayılı Siber Güvenlik Kanunu**'dur. Kanun; kritik altyapıların korunmasını, siber olaylara müdahale ekiplerinin kurulmasını, standart ve sertifikasyon rejimini düzenlemiş ve 8 Ocak 2025 tarihli 177 sayılı Cumhurbaşkanlığı Kararnamesiyle kurulan **Siber Güvenlik Başkanlığı'na** denetim, arama ve el koyma dâhil kapsamlı yetkiler tanımıştır.

İkinci dalga, 24 Temmuz 2026'da Türkiye Büyük Millet Meclisi tarafından kabul edilen ve 31 Temmuz 2026 tarihli ve 33326 sayılı Resmî Gazete'de yayımlanan **7590 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun**'dur. Bu Kanun'la internet alan adı yönetimi, internet altyapısı yönetimi ve **iletişimin tespiti ile analizi** işlevleri Bilgi Teknolojileri ve İletişim Kurumu'ndan (BTK) Siber Güvenlik Başkanlığı'na aktarılmış; ayrıca Başkanlığa, güvenlik ve istihbarat kurumlarının talebi üzerine ya da re'sen, **yargı kararını beklemeksizin** acil tedbir belirleme yetkisi tanınmıştır. Belirlenen tedbirlerin işletmeciler, erişim sağlayıcılar ve veri merkezleri tarafından

bildirimden itibaren **iki saat içinde** uygulanması zorunlu tutulmuş; tedbir yirmi dört saat içinde sulh ceza hâkimliğine sunulmakta ve hâkimin kırk sekiz saat içinde karar vermemesi hâlinde tedbir kendiliğinden ortadan kalkmaktadır.

Bu düzenleme, teknik bakımdan anlaşılabilir bir ihtiyaca dayanmaktadır: devam eden bir saldırı sırasında kötücül altyapının erişime kapatılması saatler değil dakikalar meselesidir ve klasik yargısal usul bu hıza uygun değildir. Buna karşılık aynı mekanizma, içerik ve erişim üzerinde yargı kararı olmaksızın işleyen bir müdahale imkânı yarattığından, kamuoyunda ve meslek örgütleri nezdinde yoğun eleştiriye konu olmuştur. Alternatif Bilişim Derneği, İnternet Teknolojileri Derneği, Linux Kullanıcıları Derneği, Özgür Yazılım Derneği, Pardus Kullanıcıları Derneği ile TMMOB Bilgisayar Mühendisleri Odası ve TMMOB Elektrik Mühendisleri Odası'nın ortak bildirisinde düzenleme doğrudan *internet sansürü* olarak nitelendirilmiştir (Alternatif Bilişim ve diğerleri, 2026).

Bu çalışmanın amacı, tarafların iddialarını tekrarlamak değil; düzenlemenin metnini teknik ve hukuki ölçütlerle çözümleyerek riskin nereden kaynaklandığını ve hangi güvencelerle dengelenebileceğini ortaya koymaktır. Çalışmada herhangi bir davaya, soruşturmaya ya da kişiye atıf yapılmamış olup amaç, yürürlükteki mevzuatın teknik ve hukuki bakımdan değerlendirilmesidir.

Makalenin geri kalanı şu şekilde düzenlenmiştir. İkinci bölüm, birbirinden farklı üç hukuki rejimi -- siber dayanıklılık, adli iletişimin denetlenmesi ve önleyici erişim yönetimi -- ayırt etmekte ve bunların birleştirilmesinin doğurduğu sorunu ortaya koymaktadır. Üçüncü bölüm 7545 sayılı Kanun'un mimarisini, dördüncü bölüm kurumsal yapılanma ve uygulama durumunu, beşinci bölüm ceza hükümlerini incelemektedir. Altıncı bölüm 7590 sayılı Kanun'la gelen devri ve acil tedbir mekanizmasını çözümlemekte; yedinci bölüm yargısal denetim sorununu, sekizinci bölüm Avrupa İnsan Hakları Mahkemesi ölçütlerini ele almaktadır. Dokuzuncu bölüm sansür riskini karşı argümanlarıyla birlikte tartışmakta; onuncu bölüm karşılaştırmalı çerçeveyi, on birinci bölüm adli bilişim ve bilirkişilik bakımından sonuçları sunmaktadır. On ikinci bölüm önerileri, on üçüncü bölüm sonucu içermektedir.

2. Kavramsal Çerçeve: Birbirine Karıştırılan Üç Rejim

2.1. Üç Ayrı Hukuki Rejim

Kamuoyu tartışmasında sıklıkla tek bir başlık altında toplanan işlevler, hukuken birbirinden ayrı üç rejime aittir. Bu ayrımın yapılmaması, hem düzenlemeyi savunanların hem eleştirenlerin argümanlarını bulanıklaştırmaktadır.

Birinci rejim, siber dayanıklılıktır. Kritik altyapıların saldırılara karşı korunması, zafiyet ve olay bildirimi, güvenlik standartlarının belirlenmesi, denetim ve sertifikasyon bu kapsamdadır. Muhatabı kurum ve işletmelerdir; yaptırımı esas olarak idari niteliktedir. Avrupa Birliği'nde bu alan (AB) 2022/2555 sayılı NIS2 Direktifiyle düzenlenmiştir.

İkinci rejim, adli amaçlı iletişimin denetlenmesidir. Suç şüphesine bağlı olarak, belirli bir kişi hakkında ve hâkim kararıyla iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi buraya girer. Türk hukukunda 5271 sayılı Ceza Muhakemesi

burakolgun.com

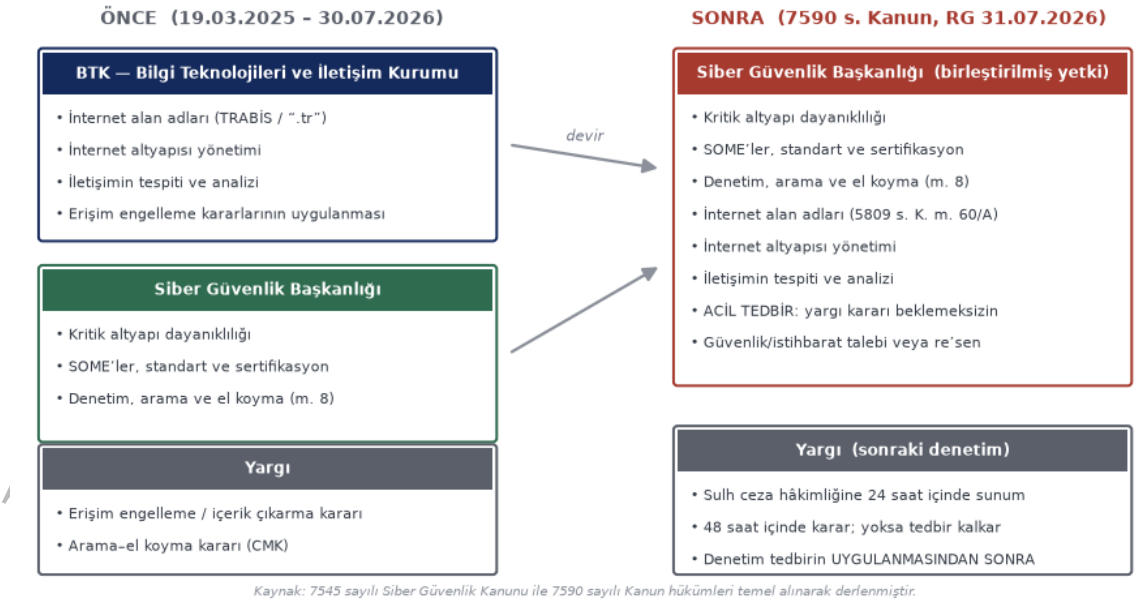
Kanunu'nun 135. maddesi, katalog suçlar, süre sınırı, hâkim kararı ve sonradan bildirim yükümlülüğü içeren ayrıntılı bir çerçeve öngörmektedir.

Üçüncü rejim, önleyici erişim yönetimidir. İçeriğin çıkarılması ya da erişimin engellenmesi, suç şüphesinden bağımsız olarak ve çoğu zaman kitlesel etki doğuracak biçimde uygulanır. Türk hukukunda 5651 sayılı Kanun bu alanı düzenler ve ifade özgürlüğüyle doğrudan temas ettiğinden anayasal denetimin en yoğun olduğu alandır.

2.2. Rejimlerin Birleştirilmesinin Doğurduğu Sorun

Bu üç rejimin ortak noktası, üçünün de aynı teknik altyapıya -- ağ trafiğine erişime, yönlendirme kontrolüne ve kayıt kapasitesine -- dayanmasıdır. Hukuki bakımdan ise meşruiyet temelleri, muhatapları, süre sınırları ve denetim usulleri birbirinden tamamen farklıdır. Bir kurumun üç rejime birden hâkim olması, teknik verimlilik bakımından avantaj sağlarken hukuki bakımdan **güvence seviyelerinin en düşük olana doğru yakınsaması** riskini doğurur.

Bu yakınsama şöyle işler: idari verimlilik gerekçesiyle dayanıklılık rejimi için tasarlanan hızlı usul, giderek erişim yönetimi kararlarında da uygulanmaya başlar. Dayanıklılık rejiminde hız meşru bir gerekliliktir; erişim yönetiminde ise aynı hız, ifade özgürlüğüne yönelik müdahalenin yargısal denetimden kaçmasına yol açar. Literatürde **amaç kayması** (function creep) olarak adlandırılan bu olgu, gözetim yetkilerinin tarihsel gelişiminde düzenli olarak gözlenen bir örüntüdür.



Şekil 1. 7590 sayılı Kanun öncesi ve sonrasında yetkilerin kurumsal dağılımı

Şekil 1'de görüldüğü üzere, devir öncesinde üç işlev üç ayrı odakta bulunmaktaydı: dayanıklılık Siber Güvenlik Başkanlığı'nda, alan adı ve iletişim altyapısı BTK'da, erişim engelleme ve arama–el koyma kararları ise yargıdaydı. Devir sonrasında ilk iki küme tek bir idari birimde toplanmış; yargının konumu ise **önceden karar veren merci** olmaktan çıkıp **sonradan onaylayan merci** hâline gelmiştir. Yapısal değişim tam olarak buradadır.

3. 7545 Sayılı Kanun'un Mimarisi

3.1. Amaç, Kapsam ve Tanımlar

Kanun'un 1. maddesi amacı, siber uzaydaki millî gücü oluşturan unsurlara karşı tehditlerin tespit ve bertaraf edilmesi ile siber olayların etkilerini azaltmaya yönelik esasların belirlenmesi olarak tanımlamaktadır. 2. madde kapsamı siber uzayda faaliyet gösteren kamu kurum ve kuruluşları, meslek kuruluşları ile gerçek ve tüzel kişiler olarak belirlemekte; **istihbari faaliyetleri kapsam dışında** bırakmaktadır. Bu istisna önemlidir: istihbarat faaliyetleri 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu rejimine tabi kalmaktadır.

3. maddedeki tanımlar arasında kritik altyapı, kesintiye uğraması hâlinde can kaybına veya büyük ekonomik zarara yol açabilecek sistemler olarak tarif edilmektedir. Ancak hangi sektörlerin kritik altyapı sayılacağı Kanun metninde sayılmamış, ikincil düzenlemeye bırakılmıştır. Bu, kapsamın idari işlemle genişletilebilmesi anlamına gelmekte ve **hukuki belirlilik** bakımından ilk tartışma başlığını oluşturmaktadır.

3.2. Başkanlığın Görev ve Yetkileri

Kanun'un 5. maddesi Başkanlığın görevlerini; kritik altyapıların koruma ve dayanıklılığını artırmak, siber olaylara müdahale ekiplerini (SOME) kurmak ve denetlemek, siber güvenlik standartlarını hazırlamak, test ve sertifikasyon işlemlerini yürütmek olarak saymaktadır.

6. madde ise yetkileri düzenlemektedir. Buna göre Başkanlık; bilişim sistemlerine uygun yazılım ve donanım kurulumunu sağlayabilir, siber olaya maruz kalanlara yerinde veya uzaktan müdahale desteği verebilir, ihtiyaç hâlinde bilgi, belge ve veri talep edebilir ve bunları **en fazla iki yıl** muhafaza edebilir, log kayıtlarını toplayıp değerlendirebilir. Maddenin ikinci fıkrası, kişisel verilerin belirli, açık ve meşru amaçlarla işleneceğini; erişilmesini gerektiren sebepler ortadan kalktığında silineceğini, yok edileceğini veya anonim hâle getirileceğini öngörmektedir.

Buradaki iki yıllık azami saklama süresi, veri minimizasyonu ilkesi bakımından olumlu bir sınırdır. Buna karşılık *ihtiyaç hâlinde bilgi, belge ve veri talep etme* yetkisinin sınırlarının maddede daraltılmamış olması, uygulamada geniş yorumlanmaya elverişlidir. Talebin hangi eşiğe bağlı olduğu -- somut bir siber olay mı, genel bir risk değerlendirmesi mi -- metinden açıkça anlaşılmamaktadır.

3.3. Yükümlülükler

Kanun'un 7. maddesi, kapsamdakilere; Başkanlığın talep ettiği veri ve belgeleri zamanında sağlamak, zafiyet ve siber olayları gecikmeksizin bildirmek, yetkilendirilmiş siber güvenlik uzmanlarından tedarik yapmak ve sertifikasyon onayı almak yükümlülükleri getirmektedir. Bu yükümlülükler 19 Mart 2025'ten itibaren yürürlüktedir; ancak bildirimin hangi süre içinde ve hangi biçimde yapılacağı gibi uygulama ayrıntıları ikincil düzenlemeye bırakılmıştır.

burakoguz.com

3.4. Denetim, Arama ve El Koyma

Kanun'un 8. maddesi, teknik bakımdan en tartışmalı hükümdür. Maddenin dördüncü fıkrası denetimle görevlendirilenlere elektronik ortamdaki verinin, belgelerin ve elektronik altyapının incelenmesi, kopya alınması ve dijital suret çıkarılması yetkisi tanımaktadır.

Beşinci fıkra ise arama ve el koymayı düzenlemektedir. Buna göre millî güvenlik, kamu düzeni veya suç işlenmesinin önlenmesi amacıyla hâkim kararıyla ya da gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emriyle arama yapılabilir; uzun süreli hizmet aksamasına yol açmayacak şekilde kopya çıkarılabilir ve el konulabilir. Hâkim kararı olmaksızın yapılan işlem **yirmi dört saat içinde** hâkimin onayına sunulur, hâkim **kırk sekiz saat içinde** karar verir. Veri merkezi işletmecileri bakımından yalnızca hâkim kararıyla işlem yapılabilirken, **kamu kurum ve kuruluşları bakımından hâkim kararı aranmamaktadır**.

Bu kurgu, ceza muhakemesindeki genel rejimle karşılaştırıldığında iki bakımdan ayrışmaktadır. Birincisi, arama sebebi *suç şüphesi* değil, millî güvenlik ve kamu düzeni gibi **önleyici** kavramlara bağlanmıştır; bu kavramların kapsamı ceza muhakemesindeki şüphe eşiğine göre çok daha geniştir. İkincisi, kamu kurumları bakımından yargısal denetimin tümüyle devre dışı bırakılması, kamu kurumlarında bulunan vatandaşa ait verilerin de aynı rejime tabi olması sonucunu doğurmaktadır. Vatandaşın sağlık, vergi veya sosyal güvenlik verisi, kurum nezdinde tutulduğu için hâkim kararı olmaksızın incelenebilecek hâle gelmektedir. Verinin kime ait olduğu ile nerede tutulduğu farklı meselelerdir; hükmün bu ayrımı gözetmemesi teknik değil hukuki bir eksikliktir.

4. Kurumsal Yapılanma ve Uygulama Durumu

Siber Güvenlik Başkanlığı, 8 Ocak 2025 tarihli ve 177 sayılı Cumhurbaşkanlığı Kararnamesiyle kurulmuştur. 7545 sayılı Kanun 19 Mart 2025'te yürürlüğe girmiş; ilk Siber Güvenlik Başkanı 24 Ekim 2025 tarihinde atanmıştır. 25 Aralık 2025 tarihli ve 192 sayılı Cumhurbaşkanlığı Kararnamesiyle teşkilat yapısı genişletilmiş ve kadro sayısı 135'ten 204'e yükseltilmiştir. 21 Ağustos 2026 tarihli ve 33347 sayılı Resmî Gazete'de ise Başkanlığın 275 sözleşmeli personel alımına ilişkin duyurusu yayımlanmıştır. Bu sıralama, kurumun hâlâ **kuruluş ve kadrolaşma evresinde** olduğunu göstermektedir.

Buna karşılık ikincil mevzuat tarafında tablo aynı hızda ilerlememiştir. Kanun, tüm ikincil düzenlemelerin **19 Mart 2026**'ya kadar yürürlüğe girmesini öngörmüştü. Kanun'un yürürlüğe girmesinden dokuz ay sonra yapılan bir değerlendirmede; siber olay bildirimi ve log yönetimi usulleri, güvenlik politikası ve belge standartları, sertifikasyon ve yetkilendirme usulleri, teknik kriterler, bağımsız denetim mekanizması, SOME kurulması ve işleyişi ile Siber Güvenlik Kurulu çalışma usullerine ilişkin düzenlemelerin henüz yayımlanmadığı; kritik altyapı sektörlerinin de resmen belirlenmediği tespit edilmiştir (Forseti, 2025).

Bu tablo, düzenlemenin bugünkü hâline ilişkin dikkat çekici bir asimetriye işaret etmektedir: **yetkiler yürürlüktedir, yükümlülüklerin içeriği ise henüz belirsizdir.** Yükümlü kuruluşlar bakımından bu durum, hangi davranışın ihlâl sayılacağını önceden bilememe sorunu doğurur. Ceza ve idari para cezası öngören bir rejimde bu belirsizlik, yalnızca pratik bir güçlük değil, kanunilik ilkesi bakımından da tartışma konusudur.

burakolgun.com

İkinci bir sonuç, kurumsal kapasiteyle yetki genişliği arasındaki mesafedir. Kadrosu iki yüzlü rakamlarla ifade edilen ve teşkilatlanmasını yeni tamamlamakta olan bir Başkanlığa; kritik altyapı denetiminin yanı sıra alan adı yönetimi, internet altyapısı ve iletişimin tespiti ile analizi gibi son derece teknik ve yüksek hacimli işlevlerin aynı anda devredilmesi, uygulamada **yetkinin fiilen alt birimlerce ve rutin usullerle** kullanılması sonucunu doğurabilir. Yetki ne kadar geniş, denetim kapasitesi ne kadar sınırlıysa, kararların bireyselleştirilmesi o kadar zayıflar.

5. Ceza Hükümleri ve Belirlilik Sorunu

5.1. Öngörülen Yaptırımlar

Kanun'un 16. maddesi, siber güvenlik alanında Türk hukukunun gördüğü en ağır yaptırım kataloglarından birini içermektedir. Tablo 1 bu yaptırımları özetlemektedir.

Tablo 1. 7545 sayılı Kanun'un 16. maddesinde öngörülen yaptırımlar

Fiil	Yaptırım
Talep edilen bilgi veya belgeyi vermemek	1-3 yıl hapis + 500-1.500 gün adli para cezası
Onay almaksızın faaliyet yürütmek	2-4 yıl hapis + 1.000-2.000 gün adli para cezası
Sır saklama yükümlülüğünü ihlâl etmek	4-8 yıl hapis
Veri sızıntısı olmadığını bilerek asılsız içerik üretmek veya yaymak	2-5 yıl hapis
Türkiye'nin siber millî gücünü oluşturan unsurlara saldırmak	8-12 yıl hapis
Saldırı sonucu elde edilen veriyi yaymak veya satmak	10-15 yıl hapis
12. maddeye aykırı davranmak	3-5 yıl hapis
Görevi kötüye kullanmak	1-3 yıl hapis
7. maddedeki sorumlulukları yerine getirmemek (idari)	1.000.000 - 10.000.000 TL
18. maddedeki sorumlulukları yerine getirmemek (idari)	10.000.000 - 100.000.000 TL

Not. Kaynak: 7545 sayılı Siber Güvenlik Kanunu'nun 16. maddesi temel alınarak yazar tarafından derlenmiştir. Tablo özet niteliğinde olup uygulamada madde metni esastır.

5.2. Veri Sızıntısı Fıkrası: Unsurlar ve Sınırlar

Kataloğun en çok tartışılan hükmü, siber güvenlikle ilgili veri sızıntısı olmadığını bilmesine rağmen, kamuoyunda panik yaratmak veya kurum ya da kişileri hedef almak amacıyla asılsız içerik üretilmesini ya da yayılmasını iki yıldan beş yıla kadar hapis cezasıyla cezalandıran fıkradır. Yasama sürecinde hükmün kapsamı daraltılmış ve *veri sızıntısı* ibaresi *siber güvenlikle ilgili veri sızıntısı* olarak değiştirilmiştir; ancak bu değişikliğin temel kaygıları gidermediği yönünde eleştiriler sürmüştür.

Hükmün suç tipi olarak üç unsuru bulunmaktadır:

- **Maddi unsur:** asılsız içeriğin üretilmesi veya yayılması,
- **Manevi unsur:** sızıntının bulunmadığının *bilinmesi* (doğrudan kast),
- **Özel kast:** kamuoyunda panik yaratma ya da kurum veya kişileri hedef alma amacı.

Metin düzeyinde bu unsurlar hükmü belirli ölçüde sınırlamaktadır: iyi niyetle, doğruluğuna inanarak yapılan bir paylaşım tipiklik unsurunu karşılamayacaktır. Sorun, metin düzeyinde değil **uygulama düzeyinde** ortaya çıkmaktadır.

burakcelik.com

5.3. Caydırıcı Etki

Bir veri sızıntısı iddiasının doğruluğu, çoğu zaman ancak inceleme sonucunda anlaşılabilir. Güvenlik araştırmacısı ya da gazeteci, elindeki veri kümesinin gerçek bir sızıntıdan mı yoksa daha önce açığa çıkmış kayıtların yeniden derlenmesinden mi kaynaklandığını paylaşım anında kesin olarak bilemeyebilir. Bu belirsizlik, **hakkında soruşturma açılma ihtimalinin kendisini** bir caydırıcı unsura dönüştürür. Ceza hukukunda *chilling effect* olarak adlandırılan bu olgu, mahkûmiyetle değil, yargılanma riskiyle işler.

Bu etkinin somut sonucu, sızıntı ihbarlarının kamuoyuyla değil yalnızca kurumlarla paylaşılmasına yönelme; sorumlu açıklama (responsible disclosure) pratiğinin ise kurumun yanıt vermemesi hâlinde tıkanmasıdır. Nitekim hükme yönelik eleştiriler, Türkiye Gazeteciler Sendikası, İfade Özgürlüğü Derneği, Medya ve Hukuk Çalışmaları Derneği ile uluslararası kuruluşlar tarafından gazetecilik faaliyeti ve mahremiyet bakımından dile getirilmiştir. Dengeleyici çözüm, hükmü tümüyle kaldırmak yerine, iyi niyetli güvenlik araştırması ve gazetecilik faaliyeti bakımından açık bir **hukuka uygunluk sebebi** öngörmektir. Karşılaştırmalı hukukta bu tür güvenli liman düzenlemeleri, zafiyet bildirimini teşvik ettiği için siber güvenliği zayıflatmaz, aksine güçlendirir.

6. 7590 Sayılı Kanunla Gelen Devir

6.1. Düzenleme Tekniği: Torba Kanun

7590 sayılı Kanun, adından da anlaşılacağı üzere birden çok kanunda değişiklik yapan bir *torba kanun*dur. Aynı Kanun; turizm ve imalat sektörüne destek, asgari emekli aylığının artırılması, vergi, sosyal güvenlik, kamu ihale sistemi, ulaştırma ve eğitim alanlarında düzenlemeler içermektedir. İletişim altyapısı ve iletişimin tespiti ile analizi gibi temel hak ve özgürlüklerle doğrudan bağlantılı bir yetki devrinin, bu kapsamdaki bir kanunun içinde düzenlenmesi, **yasama tekniği bakımından başlı başına bir eleştiri konusudur**.

Torba kanun yöntemi, düzenlemenin kendi konusu bakımından ayrı ve derinlemesine görüşülmesini fiilen imkânsızlaştırır. Bir hükmün Genel Kurul'da ne kadar tartışıldığı, sonradan yapılacak anayasallık denetiminde doğrudan bir ölçüt olmasa da; kamuoyunun bilgilenme imkânı, paydaş görüşlerinin alınması ve düzenlemenin olgunlaşması bakımından belirleyicidir. Temel haklara etki eden düzenlemelerin müstakil kanunlarla yapılması, usul ekonomisi değil demokratik meşruiyet meselesidir.

6.2. Devredilen Yetkiler

Kanun'un 21. maddesiyle BTK'nın yetkileri Siber Güvenlik Başkanlığı'na aktarılmıştır. Devrin kapsamı üç ana başlıkta toplanmaktadır:

- **İnternet alan adı yönetimi.** 5809 sayılı Elektronik Haberleşme Kanunu'na eklenen 60/A maddesiyle internet alan adlarına ilişkin strateji ve politikaların belirlenmesi ile bu alanda düzenleme yapma yetkisi Başkanlığa verilmiş; BTK'nın alan adlarına ilişkin görevleri kaldırılmıştır.
- **İnternet altyapısı yönetimi.** Veri merkezleri ve teknik altyapıya ilişkin yetkiler Başkanlık bünyesinde toplanmıştır.

burakolgun.com

- **İletişimin tespiti ve analizi.** Elektronik haberleşme trafiğine ilişkin tespit ve analiz işlevi Başkanlığa aktarılmıştır.

Ayrıca 5651 sayılı Kanun'daki BTK atıfları Siber Güvenlik Başkanlığı olarak değiştirilmiş; 7545 sayılı Kanun'a eklenen geçici maddeyle BTK'dan Başkanlığa personel, varlık ve altyapı devri düzenlenmiştir. Böylece 5651 sayılı Kanun kapsamındaki erişim engelleme ve içerik çıkarma kararlarının **uygulayıcısı** da Başkanlık hâline gelmiştir.

Alan adı yönetiminin devri, ilk bakışta teknik bir düzenleme gibi görünse de sonuçları bakımından önemlidir. Alan adı sistemine hâkim olan merci, bir alan adının çözümlenip çözümlenmeyeceğini belirleyebilir; bu ise erişim engellemenin en hızlı ve en geniş etki doğuran teknik yöntemidir. Alan adı yönetimi, iletişim altyapısı ve erişim tedbiri yetkisinin aynı elde toplanması, teknik zincirin **tüm halkalarının** tek bir idari iradeye bağlanması anlamına gelmektedir.

Tablo 2. 7590 sayılı Kanun'la yetki dağılımında meydana gelen değişim

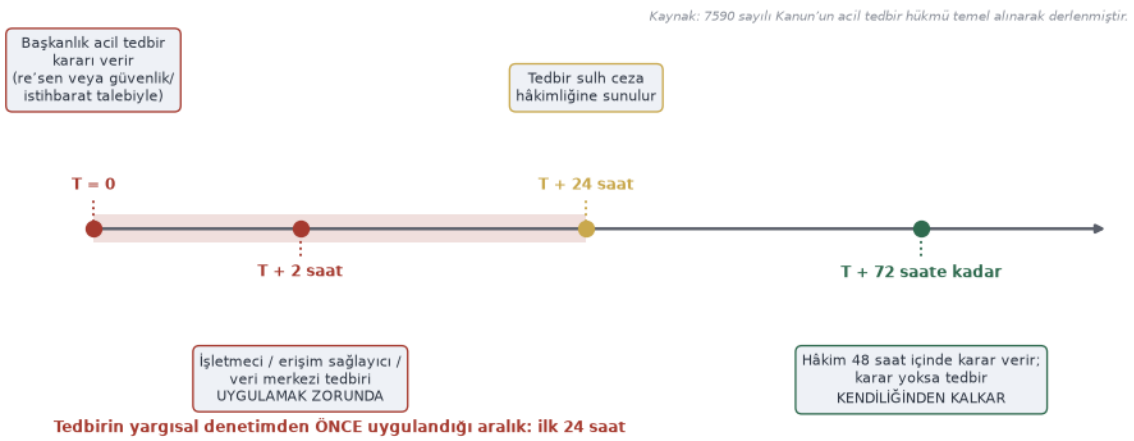
İşlev	Devir öncesi	Devir sonrası	Denetim niteliği
Kritik altyapı dayanıklılığı, SOME, sertifikasyon	Siber Güvenlik Başkanlığı	Siber Güvenlik Başkanlığı	İdari denetim
İnternet alan adları (".tr") yönetimi	BTK	Siber Güvenlik Başkanlığı (5809 s. K. m. 60/A)	İdari düzenleme
İnternet altyapısı ve veri merkezleri	BTK	Siber Güvenlik Başkanlığı	İdari düzenleme
İletişimin tespiti ve analizi	BTK	Siber Güvenlik Başkanlığı	Kanunda ayrıntılı güvence yok
Erişim engelleme / içerik çıkarma kararının uygulanması	BTK (yargı kararı üzerine)	Siber Güvenlik Başkanlığı	Yargı kararına bağlı
Acil tedbir belirleme	Yok (yargı kararı gerekli)	Siber Güvenlik Başkanlığı (re'sen veya talep üzerine)	Sonradan hâkim onayı (24 + 48 saat)
Arama ve el koyma (7545 s. K. m. 8)	Siber Güvenlik Başkanlığı	Siber Güvenlik Başkanlığı	Hâkim kararı; kamu kurumlarında aranmaz

Not. Kaynak: 7545 ve 7590 sayılı Kanun hükümleri ile ilgili kurumsal duyurular temel alınarak yazar tarafından derlenmiştir.

6.3. Acil Tedbir Mekanizması

Düzenlemenin merkezinde acil tedbir mekanizması bulunmaktadır. Başkanlık, güvenlik ve istihbarat kurumlarının talebi üzerine ya da re'sen, yargı kararını beklemeksizin tedbir belirleyebilmektedir. Belirlenen tedbir işletmecilere, erişim sağlayıcılara, veri merkezlerine ya da ilgili içerik ve yer sağlayıcılara derhâl bildirilir ve bildirimden itibaren **en geç iki saat içinde** uygulanması zorunludur. Tedbir **yirmi dört saat içinde** sulh ceza hâkimliğine sunulur; hâkim **kırk sekiz saat içinde** karar verir. Karar verilmemesi hâlinde tedbir kendiliğinden ortadan kalkar.

burakkurt.com



Şekil 2. Acil tedbir mekanizmasının işleyişi ve süreler

Şekil 2, mekanizmanın kritik özelliğini görünür kılmaktadır: tedbirin uygulanması ile yargısal denetimin başlaması arasında **yirmi dört saatlik bir aralık** bulunmaktadır ve bu aralık boyunca müdahale tam olarak yürürlüktedir. Hâkimin karar süresi de eklendiğinde yargısal denetimin tamamlanması yetmiş iki saati bulabilmektedir.

Mekanizmanın kendiliğinden sona erme kuralı, tasarımda yer alan olumlu bir güvencedir; hâkimin sessiz kalması hâlinde tedbirin sürmesini engeller. Ancak bu güvence, internet ortamındaki müdahalelerin niteliği düşünüldüğünde sınırlı bir koruma sağlar. Bir içeriğin ya da hizmetin yetmiş iki saat erişime kapalı kalması, birçok olayda müdahalenin amacına ulaşması için yeterlidir; haber değeri taşıyan bir içerik bakımından bu süre, içeriğin güncelliğini yitirmesine yeter. Dolayısıyla **tedbirin sonradan kaldırılması, doğurduğu etkiyi geriye dönük olarak ortadan kaldırmaz.**

İki saatlik uygulama süresi de teknik bakımdan değerlendirilmelidir. Süre, gerçek bir saldırı senaryosunda makul ve hatta gerekli olabilir. Buna karşılık aynı süre, işletmecinin tedbirin hukuka uygunluğunu değerlendirmesine, hukuki görüş almasına ya da itiraz etmesine imkân bırakmaz. İşletmeci bakımından pratik sonuç, **tedbiri sorgusuz uygulamak** dışında bir seçeneğin bulunmamasıdır. Aracı kuruluşların hukuka aykırı talepler karşısında direnç gösterebilmesi, ifade özgürlüğünün korunmasında önemli bir yapısal güvencedir; bu sürenin bu güvenceyi fiilen ortadan kaldırdığı söylenebilir.

7. Yargısal Denetim Sorunu

7.1. Önceki Denetim ile Sonraki Denetim Arasındaki Fark

Temel hak ve özgürlüklere yönelik müdahalelerde yargısal denetimin **zamanlaması**, denetimin varlığı kadar önemlidir. Önceden yapılan denetim, müdahalenin gerçekleşmesini engelleyebildiği için koruyucudur; sonradan yapılan denetim ise ancak müdahalenin sürmesini engelleyebilir. İfade özgürlüğü alanında bu ayrım özellikle belirleyicidir; çünkü bir içeriğin belirli bir an için erişime kapatılması, çoğu zaman kalıcı olarak kapatılmasıyla benzer sonuç doğurur.

burakolgun.com

Acil tedbir mekanizması, tanım gereği sonraki denetim modelini benimsemektedir. Bunun gerekçesi hızdır ve bu gerekçe siber olay müdahalesi bakımından savunulabilirdir. Sorun, aynı mekanizmanın **hangi hâllerde kullanılabileceğinin dar biçimde tanımlanmamış olmasıdır**. Mekanizma yalnızca devam eden bir siber saldırının durdurulmasıyla sınırlı tutulsaydı, hız gerekçesi ile hak güvencesi arasında denge kurulabilirdi. Yetkinin genel ifadelerle düzenlenmesi, aynı hızlı usulün içerik temelli müdahalelerde de kullanılabilmesine imkân tanımaktadır.

7.2. Sulh Ceza Hâkimliği Modeline Yönelik Eleştiriler

Tedbirin sunulacağı merci sulh ceza hâkimliğidir. Bu hâkimliklerin kararlarına karşı itirazın yine sulh ceza hâkimliklerince incelenmesi -- yani kapalı bir itiraz devresi oluşması -- doktrinde ve uluslararası raporlarda uzun süredir eleştirilmektedir. Eleştirinin özü, itiraz merciinin farklı bir yargı düzeyi olmamasının, içtihat birliğini ve etkili denetimi zayıflattığıdır.

Bu yapısal eleştiri, acil tedbir mekanizmasının denetimi bakımından ayrıca önem kazanmaktadır. Kırk sekiz saatlik karar süresi içinde, teknik bakımdan karmaşık bir tedbirin -- örneğin bir alan adının çözümlenmemesi ya da belirli bir trafiğin engellenmesi -- gerekliliğinin ve orantılılığının değerlendirilmesi beklenmektedir. Bu değerlendirme için hâkimin teknik uzmanlık desteğine erişimi konusunda Kanun bir düzenleme içermemektedir. Uygulamada bu, denetimin **biçimsel bir onay** hâline gelmesi riskini doğurur.

7.3. Anayasa Mahkemesi'nin 5651 Sayılı Kanun İçtihadı

Türk anayasa yargısı, internet ortamındaki müdahalelere ilişkin olarak dikkate değer bir içtihat oluşturmuştur. Anayasa Mahkemesi, 11 Ekim 2023 tarihli ve E.2020/76, K.2023/172 sayılı kararıyla 5651 sayılı Kanun'un kişilik haklarının ihlâline ilişkin 9. maddesinin birinci, üçüncü, beşinci, sekizinci, dokuzuncu, onuncu ve on birinci fıkralarını iptal etmiş; iptal edilen hükümler diğer fıkraların uygulanmasını imkânsız kıldığından maddenin tamamı iptal edilmiştir. İptal kararı 10 Ekim 2024'te yürürlüğe girmiştir (AYM, E.2020/76, K.2023/172).

Kararın gerekçesi, mevcut tartışma bakımından doğrudan yol göstericidir. Mahkeme, kişilik haklarının ihlâli iddiasına dayalı olarak içeriğin çıkarılması veya erişimin engellenmesini öngören düzenlemenin, **ifade ve basın özgürlüğüne orantısız bir sınırlama** getirdiği sonucuna varmıştır. Bir başka deyişle, meşru bir amaca (kişilik haklarının korunmasına) dayanan bir tedbir dahi, usuli güvenceleri yetersizse anayasaya aykırı bulunabilmektedir.

Bu içtihat, acil tedbir mekanizması bakımından şu ölçütü ortaya koymaktadır: müdahalenin amacının meşruluğu tek başına yeterli değildir; müdahalenin **kapsamı, süresi, bireyselleştirilmesi ve etkili başvuru yolunun bulunup bulunmadığı** ayrıca değerlendirilir. Anayasa Mahkemesi'nin daha önceki bireysel başvuru kararlarında -- sosyal ağ platformlarının bütünüyle erişime kapatılmasına ilişkin kararlar dâhil -- kitlesel etki doğuran engellemeleri ifade özgürlüğü ihlâli saydığı da hatırlanmalıdır.

burakolgun.com

8. Avrupa İnsan Hakları Mahkemesi Ölçütleri Karşısında Değerlendirme

8.1. Gizli Gözetimde Asgari Güvenceler

Avrupa İnsan Hakları Mahkemesi, iletişimin gizli biçimde denetlenmesine ilişkin içtihadında, iç hukukun taşıması gereken asgari güvenceleri belirlemiştir. Weber ve Saravia kararında formüle edilen ve sonraki kararlarda geliştirilen bu ölçütler; tedbirin uygulanabileceği hâllerin niteliğinin belirlenmesi, kapsama girecek kişi kategorilerinin tanımlanması, tedbirin azami süresine ilişkin sınır konulması, elde edilen verinin incelenmesi, saklanması ve imhası usulünün düzenlenmesi, üçüncü kişilere aktarımda uygulanacak güvencelerin belirlenmesi ve verinin imha edileceği hâllerin gösterilmesi başlıklarını içermektedir (Weber ve Saravia, 2006).

Roman Zakharov kararında Mahkeme, bir gözetim sisteminin **soyut olarak** dahi incelenebileceğini; sistemin kötüye kullanıma karşı yeterli ve etkili güvenceler içermemesi hâlinde, başvurucunun kendisine yönelik somut bir tedbir gösteremese bile ihlâl tespit edilebileceğini kabul etmiştir (Roman Zakharov, 2015). Szabó ve Vissy kararında ise millî güvenlik gerekçesiyle tanınan geniş yetkilerin, **yeterince bireyselleştirilmiş şüphe** ve **bağımsız -- tercihen yargısal -- önceden izin** gerektirdiği vurgulanmıştır (Szabó ve Vissy, 2016). Big Brother Watch kararında Büyük Daire, toplu ele geçirme rejimleri bakımından **uçtan uca güvenceler** yaklaşımını benimsemiş; sürecin her aşamasında bağımsız denetim ve sonradan gözden geçirme aranmıştır (Big Brother Watch, 2021).

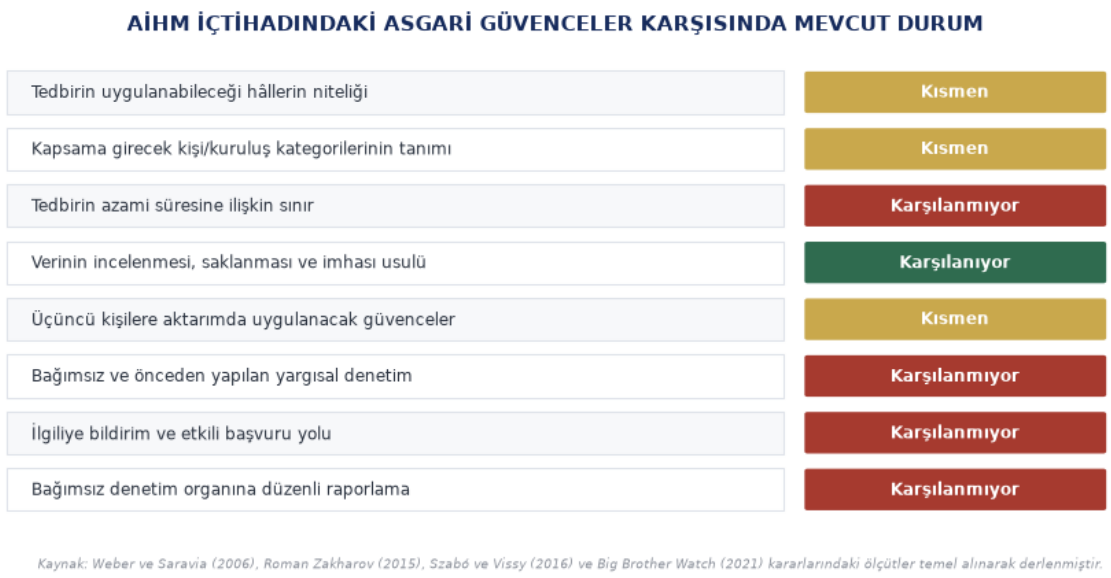
8.2. Erişim Engellemeye İlişkin İçtihat

İfade özgürlüğü boyutunda Mahkeme, Türkiye'ye ilişkin iki temel kararında ölçütlerini ortaya koymuştur. Ahmet Yıldırım kararında, tek bir içerik nedeniyle bir barındırma hizmetinin tamamına erişimin engellenmesi, öngörülebilirlik ve orantılılık ölçütlerini karşılamadığı gerekçesiyle 10. maddenin ihlâli sayılmıştır (Ahmet Yıldırım, 2012). Cengiz ve diğerleri kararında ise bir video paylaşım platformunun bütünüyle erişime kapatılması aynı yönde değerlendirilmiştir (Cengiz ve diğerleri, 2015).

Bu kararlardan çıkan ortak ölçüt, **kolektif etki** ölçütüdür: müdahalenin hedefi belirli bir içerik olsa dahi, teknik yöntemin zorunlu sonucu olarak hedef dışı içeriklerin de erişilemez hâle gelmesi, orantılılığı ortadan kaldırır. Alan adı düzeyinde ya da altyapı düzeyinde uygulanan tedbirler, teknik nitelikleri gereği tam da bu sonucu doğurmaya elverişlidir.

Şekil 3'teki değerlendirme, kanun metni esas alınarak yapılmıştır ve ikincil düzenlemelerle güvencelerin güçlendirilmesi hâlinde değişebilir. Tabloda öne çıkan üç boşluk şunlardır: tedbirin **azami süresine ilişkin bir sınır** öngörülmemiş olması, **ilgiliye bildirim ve etkili başvuru yolunun** düzenlenmemiş olması ve **bağımsız bir denetim organına düzenli raporlama** yükümlülüğünün bulunmamasıdır. Bu üç unsur, AİHM içtihadında kötüye kullanımı önleyen çekirdek güvenceler olarak kabul edilmektedir; üçünün birden bulunmaması, sistemi soyut denetim bakımından kırılgan hâle getirir.

burakolgun.com



Şekil 3. AİHM içtihadındaki asgari güvenceler karşısında mevcut düzenlemenin durumu (yazarın değerlendirmesi)

9. Sansür Riski: Kaynağı, Sınırları ve Karşı Argümanlar

9.1. Riskin Kaynağı Nedir?

Bir düzenlemenin sansür aracına dönüşme riski, çoğunlukla düzenleyicinin niyetinden değil, **tasarımın kendisinden** doğar. Hukuk devletinde bir yetkinin değerlendirilmesi, onu kullanacak kişilerin iyi niyetine göre değil, kötüye kullanılması hâlinde hangi engellerle karşılaşacağına göre yapılır. Bu ölçütle bakıldığında, incelenen düzenlemede riski artıran dört yapısal unsur bulunmaktadır.

- **Yetkinin konu bakımından sınırının dar çizilmemiş olması.** Acil tedbirin yalnızca devam eden siber saldırıların durdurulmasıyla sınırlı olduğu metinde açık biçimde belirtilmediğinden, aynı usul içerik temelli müdahalelerde de kullanılabilir.
- **Teknik zincirin tek elde toplanması.** Alan adı yönetimi, internet altyapısı, iletişimin tespiti ve tedbirin uygulanması aynı idari birimde birleştiğinde, müdahalenin teknik olarak durdurulabileceği bir ara nokta kalmaz.
- **Yargısal denetimin sonraya bırakılması.** Yirmi dört saatlik sunum ve kırk sekiz saatlik karar süresi, denetimin müdahale sonrasına ötelenmesi anlamına gelir; bu süre birçok olayda müdahalenin amacına ulaşması için yeterlidir.
- **Şeffaflık yükümlülüğünün bulunmaması.** Kaç tedbir uygulandığı, kaçının hâkim onayından geçtiği, kaçının kendiliğinden kalktığı düzenli olarak yayımlanmadığında, yetkinin nasıl kullanıldığı kamuoyunca değerlendirilemez.

9.2. Amaç Kayması Olgusu

Gözetim ve erişim kontrolü yetkilerinin tarihsel gelişimi, bu yetkilerin nadiren daraldığını; genellikle ilk tanındıkları amaçtan daha geniş alanlarda kullanılmaya başlandığını göstermektedir. Amaç kayması, kural olarak açık bir hukuk ihlâliyle değil, **mevcut yetkinin geniş yorumlanmasıyla** gerçekleşir. Terörle mücadele ya da çocuk istismarıyla mücadele

burakolgun.com

gerekçesiyle kurulan teknik altyapıların zamanla farklı içerik kategorilerine uygulanması, karşılaştırmalı hukukta çok sayıda örneği bulunan bir örüntüdür.

İncelenen düzenlemede amaç kayması riskini artıran özgün unsur, tedbirin **güvenlik ve istihbarat kurumlarının talebi üzerine** de belirlenebilmesidir. Bu, siber güvenlik gerekçesiyle kurulan hızlı usulün, siber güvenlikle doğrudan ilgisi bulunmayan taleplerin uygulanmasında da kullanılabilmesine imkân tanıyan bir kanaldır. Talebin siber güvenlikle bağlantısının hangi ölçütle denetleneceği düzenlemede belirtilmemiştir.

9.3. Karşı Argümanlar: Düzenlemeyi Savunan Gerekçeler

Değerlendirmenin dengeli olabilmesi için düzenlemeyi destekleyen gerekçelerin de ciddiyetle ele alınması gerekir.

Birincisi, hız gerekliliği gerçektir. Bir kimlik avı altyapısının, kötücül yazılım komuta-kontrol sunucusunun ya da devam eden bir hizmet dışı bırakma saldırısının kaynağının erişime kapatılması, saatler içinde yapılmadığında etkisiz kalır. Klasik yargısal usul, gecikmesinde sakınca bulunan hâller için dahi bu hıza uygun tasarlanmamıştır.

İkincisi, mekanizma sınırsız değildir. Tedbirin yirmi dört saat içinde hâkime sunulması zorunludur ve hâkimin karar vermemesi hâlinde tedbir kendiliğinden kalkar. Bu, sessizliğin idare lehine yorumlanmadığı, aksine tedbir aleyhine sonuç doğurduğu bir tasarımdır ve karşılaştırmalı hukukta rastlanan her modelden daha güvenceli değilse de, denetimsiz bir yetki de değildir.

Üçüncüsü, kurumsal birleştirmenin teknik gerekçesi vardır. Siber olay müdahalesinde tespit, analiz ve müdahale aşamalarının farklı kurumlara dağılmış olması, gerçek olaylarda koordinasyon gecikmesine yol açar. Kritik altyapı saldırılarında gecikmenin maliyeti can kaybına kadar uzanabilir.

Dördüncüsü, Türkiye tehdit yoğunluğu yüksek bir coğrafyadadır. Kamu kurumlarına ve kritik altyapılara yönelik saldırıların hacmi, düzenleyici müdahaleyi gerektirecek düzeydedir; bu yönüyle bir siber güvenlik kanunu çıkarılmış olması başlı başına olumlu bir gelişmedir.

Bu gerekçelerin hiçbiri geçersiz değildir. Ancak hepsinin ortak özelliği, **dayanıklılık rejimine** ilişkin olmasıdır. Hız gerekliliği, koordinasyon ihtiyacı ve tehdit yoğunluğu; devam eden bir saldırıya müdahaleyi haklı kılar. Bunların hiçbiri, aynı hızlı usulün içerik ve erişim üzerinde konu sınırı olmaksızın kullanılabilmesini haklı kılmaz. Sorun, yetkinin varlığı değil, **kapsamının teknik gerekçenin ötesine taşmasıdır**.

9.4. Sivil Toplumun Eleştirisi

Yedi meslek ve sivil toplum kuruluşunun ortak bildirisi, 21. maddeyi özellikle sorunlu bularak düzenlemenin internet ortamındaki işleyişi, veri akışını ve uygulamaları, sosyal ağlarda iletişim ve ifade özgürlüğünü hedef aldığını ileri sürmüştür. Bildiride iki ana eleştiri öne çıkmaktadır: Başkanlığa yargı kararını beklemeksizin önlem uygulama yetkisi verilmesi ve Başkanlığın **sınırları ile kapsamı belirsiz yetkilerle** donatılmış olması (Alternatif Bilişim ve diğerleri, 2026).

burakolgun.com

Bu eleştirilerin ilki, tasarımın kabul edilmiş bir özelliğini tespit etmektedir; tartışma, bunun gerekli ve orantılı olup olmadığındadır. İkincisi ise hukuki belirlilik ilkesine dayandığından anayasal denetim bakımından daha güçlü bir zemine sahiptir. Anayasa'nın 13. maddesi uyarınca temel hak ve özgürlükler ancak kanunla sınırlanabilir ve sınırlama ölçülü olmalıdır; kanunilik ölçütü ise yalnızca şeklî bir kanun varlığını değil, kuralın **erişilebilir, öngörülebilir ve belirli** olmasını da gerektirir.

9.5. Sanal Ağ Hizmetlerine İlişkin Tartışma

Kamuoyunda sıklıkla aynı düzenlemenin parçası gibi ele alınan bir başka konu, sanal özel ağ (Virtual Private Network — VPN) hizmetlerine ilişkin düzenleme tartışmasıdır. Gündemdeki taslak çerçevede, internet trafiğini gizlilik veya güvenlik amacıyla şifreleyerek ileten hizmetlerin *sanal ağ hizmeti*, bunları sağlayanların ise *sanal ağ hizmet sağlayıcı* olarak tanımlanması ve Türkiye'de temsilci bulundurma yükümlülüğü öngörülmesi tartışılmaktadır.

Bu konudaki değerlendirmede iki hususun ayrılması gerekir. Birincisi, söz konusu düzenlemenin **taslak aşamasında olduğu**; incelenen 7590 sayılı Kanun'un yürürlükteki metninde bu yönde bir hüküm bulunduğunun doğrulanamadığıdır. İkincisi, teknik gerçekliktir: sanal özel ağ teknolojileri yalnızca erişim kısıtlarının aşılmasında kullanılmaz; kurumsal uzaktan çalışma, banka ve sağlık verilerinin taşınması, sanayi kontrol sistemlerinin uzaktan yönetimi gibi kritik işlevlerin güvenliği doğrudan bu teknolojiye dayanır. Şifreli tünelleme kapasitesini genel olarak kısıtlayan bir düzenleme, siber güvenliği artırmak bir yana **zayıflatma** sonucu doğurur. Bu nedenle olası bir düzenlemenin, hizmetin kendisini değil belirli kullanım biçimlerini hedef alacak biçimde tasarlanması teknik bir zorunluluktur.

10. Karşılaştırmalı Çerçeve: NIS2 ve Ayrıştırma İlkesi

Avrupa Birliği'nde siber güvenlik yönetişimi, (AB) 2022/2555 sayılı NIS2 Direktifiyle düzenlenmiştir. Direktif; temel ve önemli kuruluşlar ayrımı yapmakta, risk yönetimi tedbirlerini zorunlu kılmakta, olay bildirimi için kademeli süreler öngörmekte ve üst yönetim sorumluluğu ile yüksek idari para cezaları getirmektedir.

Türkiye'deki düzenlemeyle karşılaştırıldığında en dikkat çekici fark, yaptırım düzeyinden çok **kurumsal tasarımdadır**. NIS2 rejiminde ulusal siber güvenlik otoriteleri ve olaylara müdahale ekipleri; koordinasyon, rehberlik ve denetim işlevleriyle donatılmış olup, iletişimin denetlenmesi ya da içerik engelleme yetkisi taşımazlar. Bu işlevler ayrı hukuki rejimlere ve ayrı mercilere bırakılmıştır. Ayrım, idari verimsizlik pahasına korunan bilinçli bir tercihtir; gerekçesi, güvenlik işlevinin gözetim işleviyle aynı elde toplanmasının yarattığı riski önlemektir.

Türkiye'deki tasarım ise ters yönde bir tercihi yansıtmakta; dayanıklılık, altyapı yönetimi ve iletişimin tespiti ile analizi işlevlerini tek bir Başkanlıkta birleştirmektedir. Bu tercih başlı başına hukuka aykırılık teşkil etmez; ancak birleştirmenin doğurduğu riski dengeleyecek **ek güvencelerin** öngörülmesini zorunlu kılar. Karşılaştırmalı hukukta bu güvenceler; bağımsız bir denetim komisyonu, zorunlu şeffaflık raporlaması, ilgiliye sonradan bildirim ve parlamenter denetim biçiminde kurgulanmaktadır. İncelenen düzenlemede bu araçların hiçbiri yer almamaktadır.

burakolgun.com

Tablo 3. Siber güvenlik yönetişiminde kurumsal tasarım karşılaştırması

Ölçüt	NIS2 modeli (AB)	Türkiye modeli (7545 + 7590)
Düzenlemenin konusu	Yalnızca dayanıklılık ve olay yönetimi	Dayanıklılık + altyapı yönetimi + iletişimin tespiti ve analizi
İçerik/erişim müdahalesi yetkisi	Yok — ayrı rejime bırakılmış	Var — acil tedbir mekanizması
İletişimin denetlenmesi	Ayrı hukuki rejim ve ayrı merci	Aynı Başkanlığa devredildi
Yargısal denetim	İlgili rejimin kendi usulüne tabi	Tedbir sonrası onay (24 + 48 saat)
Şeffaflık raporlaması	Öngörülmüş	Öngörülmemiş
Bağımsız denetim organı	Öngörülmüş	Öngörülmemiş
Yaptırım ağırlığı	Ağırlıklı olarak idari para cezası	Hapis cezası ağırlıklı + yüksek idari para cezası

Not. Kaynak: (AB) 2022/2555 sayılı NIS2 Direktifi ile 7545 ve 7590 sayılı Kanun hükümleri temel alınarak yazar tarafından derlenmiştir.

11. Adli Bilişim ve Bilirkişilik Bakımından Sonuçlar

Düzenlemenin uygulamaya yansıyacağı alanlardan biri de yargılama pratiğidir. Bu bölümde, teknik inceleme yapan uzman bakımından ortaya çıkan başlıca sonuçlar ele alınmaktadır.

11.1. Delil Zinciri ve İdari Yolla Elde Edilen Veri

7545 sayılı Kanun'un 8. maddesi uyarınca denetim kapsamında alınan kopyalar ve dijital suretler, idari bir işlem çerçevesinde elde edilmektedir. Bu verilerin sonradan bir ceza soruşturmasında delil olarak kullanılması hâlinde, **elde ediliş usulünün hukuka uygunluğu** ayrıca değerlendirilmesi gereken bir mesele hâline gelir. Ceza Muhakemesi Kanunu'nun 134. maddesindeki bilgisayarlarda arama, kopyalama ve el koyma rejimi ile idari denetim yetkisi farklı güvence düzeylerine sahiptir.

Teknik inceleme bakımından belirleyici olan husus, **imaj alma ve bütünlük doğrulama usulünün** kayıt altında olup olmadığıdır. Bir dijital suretin delil değeri; alındığı anın, kullanılan aracın, özet (hash) değerlerinin ve zincirin her aşamasındaki sorumlunun belgelenmesine bağlıdır. İdari denetim kapsamında alınan kopyalarda bu usulün uygulanmasını zorunlu kılan ayrıntılı bir düzenleme bulunmaması, ileride delilin güvenilirliğine yönelik itirazlara zemin hazırlayacaktır.

11.2. Acil Tedbir Kayıtlarının İncelenmesi

Acil tedbir uygulamalarına ilişkin uyuşmazlıklarda -- örneğin bir işletmecinin uygulamadan doğan zararının tazmini ya da tedbirin hukuka aykırılığının tespiti taleplerinde -- teknik inceleme, tedbirin **hangi teknik yöntemle** uygulandığına odaklanacaktır. Alan adı düzeyinde çözümleme engeli, IP düzeyinde yönlendirme kesintisi ve içerik düzeyinde filtreleme birbirinden farklı kapsam ve yan etkiler doğurur; orantılılık değerlendirmesi de bu farka göre yapılır.

Bu tür dosyalarda incelemeye esas alınacak asgari kayıtlar şunlardır:

- Tedbir bildiriminin ulaştığı **tam zaman damgası** ve uygulamaya alındığı an,
- Uygulanan **teknik yöntem** (DNS, IP, URL, protokol düzeyi) ve kapsamı,
- Tedbirin **hedef dışı etkisi**: aynı sunucu veya alan adı altındaki diğer hizmetler,
- Hâkimliğe sunum tarihi ile hâkim kararının tarihi ve **süre uyumu**,

burakolgun.com

- Tedbirin kaldırılması hâlinde **geri alma işleminin** zamanı ve bütünlüğü.

Mahkemelerce verilecek ara kararlarda bu kayıtların açıkça talep edilmesi, teknik incelemenin beyana değil kayda dayanmasını sağlayacaktır. Kayıt tutma yükümlülüğünün ikincil düzenlemelerde ayrıntılı biçimde belirlenmesi, hem idarenin hem yükümlülerin hem de yargının yararınadır.

12. Öneriler

Yukarıdaki değerlendirmeler ışığında, düzenlemenin güvenlik işlevini zayıflatmadan sansür riskini azaltacak somut öneriler aşağıda sunulmaktadır.

- **Acil tedbirin konu bakımından sınırlandırılması.** Mekanizmanın yalnızca devam eden ya da somut olarak yaklaşan siber saldırıların durdurulmasıyla sınırlı olduğu; içerik temelli müdahalelerde kullanılamayacağı kanun metninde açıkça belirtilmelidir.
- **Azami süre sınırı getirilmesi.** Hâkim onayından geçen tedbirler için de azami bir süre öngörülmeli, sürenin uzatılması gerekçeli ve ayrı bir karara bağlanmalıdır.
- **İlgiliye sonradan bildirim yükümlülüğü.** Tedbirin amacını tehlikeye düşürmeyecek aşamada, tedbire muhatap olanlara bildirim yapılması ve etkili başvuru yolunun gösterilmesi zorunlu kılınmalıdır; bu, AİHM içtihadının çekirdek güvencelerindendir.
- **Zorunlu şeffaflık raporlaması.** Uygulanan tedbir sayısı, hâkim onayından geçen ve kendiliğinden kalkan tedbirlerin oranı, uygulanan teknik yöntemlerin dağılımı ve talep kaynaklarının türü altı aylık dönemlerle yayımlanmalıdır.
- **Bağımsız denetim organı kurulması.** Yetkinin kullanımını sürekli biçimde denetleyen, teknik uzmanlık barındıran ve parlamentoya rapor sunan bağımsız bir organ öngörülmelidir.
- **Hâkimlik için teknik uzmanlık desteği.** Kırk sekiz saatlik karar süresinde teknik değerlendirme yapılabilmesi için hâkimliklere bilirkişi ya da uzman desteği sağlayan bir mekanizma kurulmalıdır.
- **Kamu kurumlarındaki kişisel veriler bakımından istisnanın daraltılması.** Kamu kurumlarında arama için hâkim kararı aranmaması kuralı, kurumda bulunan üçüncü kişilere ait kişisel veriler bakımından sınırlandırılmalıdır.
- **İyi niyetli güvenlik araştırması için hukuka uygunluk sebebi.** Zafiyet bildirimi ve sorumlu açıklama kapsamında yapılan paylaşımlar bakımından açık bir güvenli liman hükmü getirilmelidir.
- **İkincil mevzuatın gecikmeksizin tamamlanması.** Kritik altyapı sektörlerinin belirlenmesi, bildirim usulleri, kayıt tutma standartları ve bağımsız denetim mekanizması ivedilikle düzenlenmelidir.
- **Temel haklara etki eden düzenlemelerin müstakil kanunla yapılması.** Bu nitelikteki hükümlerin torba kanunlar içinde düzenlenmesinden kaçınılmalıdır.

burakolgun.com

13. Sonuç

7545 sayılı Siber Güvenlik Kanunu, Türkiye'nin uzun süredir dağınık mevzuata dayanan siber güvenlik yönetişimini müstakil bir kanuna kavuşturmuş ve kritik altyapıların korunması bakımından gerçek bir ihtiyaca karşılık vermiştir. Kanun'un çıkarılmış olması, kurumsal yapının oluşturulması ve kadrolaşmanın sürdürülmesi olumlu gelişmelerdir.

Buna karşılık düzenlemenin bugünkü hâli, üç yapısal sorun taşımaktadır. Birincisi, birbirinden farklı hukuki temellere sahip üç rejimin -- siber dayanıklılık, iletişimin denetlenmesi ve erişim yönetimi -- tek bir idari birimde toplanmasıdır. Bu birleştirme teknik verimlilik sağlarken, güvence düzeylerinin en düşük olana doğru yakınsaması riskini doğurmaktadır. İkincisi, 7590 sayılı Kanun'la getirilen acil tedbir mekanizmasında yargısal denetimin müdahale sonrasına bırakılmış olmasıdır; iki saatlik uygulama zorunluluğu ile yirmi dört saatlik sunum süresi birlikte değerlendirildiğinde, tedbirin denetimden önce tam etkisini doğurduğu bir aralık ortaya çıkmaktadır. Üçüncüsü, yetkilerin yürürlükte olmasına karşılık yükümlülüklerin içeriğini belirleyen ikincil düzenlemelerin tamamlanmamış olmasıdır.

Sansür riski bakımından varılan sonuç şudur: risk, düzenleyicinin niyetinden değil tasarımın kendisinden kaynaklanmaktadır. Acil tedbirin konu bakımından sınırının dar çizilmemesi, teknik zincirin tek elde toplanması, denetimin sonraya bırakılması ve şeffaflık yükümlülüğünün bulunmaması bir araya geldiğinde; siber güvenlik için tasarlanan bir aracın içerik denetimi için kullanılmasını hukuken engelleyen bir mekanizma kalmamaktadır. Bu tespit, yetkinin fiilen kötüye kullanıldığı iddiası değil, kötüye kullanıma karşı yapısal engel bulunmadığı tespitidir; hukuk devletinde değerlendirme ölçütü de budur.

Düzenlemeyi savunan gerekçeler -- hız gerekliliği, koordinasyon ihtiyacı ve tehdit yoğunluğu -- ciddiye alınmayı hak etmektedir; ancak bunların tamamı dayanıklılık rejimine ilişkindir ve hızlı usulün içerik ile erişim üzerinde konu sınırı olmaksızın kullanılabilmesini haklı kılmaz. Aranan denge, yetkiyi ortadan kaldırmakla değil, kapsamını teknik gerekçeyle sınırlandırmak ve kullanımını denetlenebilir kılmakla kurulabilir.

Anayasa Mahkemesi'nin 5651 sayılı Kanun'un 9. maddesine ilişkin iptal kararı, meşru amaca dayanan bir tedbirin dahi usuli güvenceleri yetersizse anayasaya aykırı bulunabileceğini göstermiştir. Avrupa İnsan Hakları Mahkemesi içtihadında aranan azami süre sınırı, ilgiliye bildirim ve bağımsız denetim güvencelerinin üçünün birden bulunmaması, mevcut düzenlemeyi hem anayasal hem de uluslararası denetim bakımından kırılgan kılmaktadır. Bu güvencelerin ikincil mevzuatla ya da kanun değişikliğiyle eklenmesi, düzenlemenin güvenlik işlevini zayıflatmayacak; aksine hukuki dayanağını ve sürdürülebilirliğini güçlendirecektir.

birakolgun.com

Kaynakça

Ahmet Yıldırım / Türkiye, B. No. 3111/10, AİHM (18 Aralık 2012).

Alternatif Bilişim Derneği, İnternet Teknolojileri Derneği, Linux Kullanıcıları Derneği, Özgür Yazılım Derneği, Pardus Kullanıcıları Derneği, TMMOB Bilgisayar Mühendisleri Odası ve TMMOB Elektrik Mühendisleri Odası. (2026). Siber Güvenlik Başkanlığı'na sınırsız yetki veren düzenleme, internet sansürüdür [Ortak bildiri]. https://www.linux.org.tr/2026/08/siber-guvenlik-baskanligina-sinirsiz-yetki-veren-duzenleme-internet-sansurudur/

Anayasa Mahkemesi. (2023). E.2020/76, K.2023/172, 11/10/2023 (5651 sayılı Kanun'un 9. maddesinin iptali). Resmî Gazete (10 Ocak 2024).

Avrupa Birliği. (2022). Birlik genelinde yüksek ortak siber güvenlik düzeyine ilişkin (AB) 2022/2555 sayılı Direktif (NIS2). Avrupa Birliği Resmî Gazetesi, L 333/80. http://data.europa.eu/eli/dir/2022/2555/oj

Big Brother Watch ve diğerleri / Birleşik Krallık [BD], B. No. 58170/13, 62322/14 ve 24960/15, AİHM (25 Mayıs 2021).

Cengiz ve diğerleri / Türkiye, B. No. 48226/10 ve 14027/11, AİHM (1 Aralık 2015).

Cumhurbaşkanlığı. (2025a). Siber Güvenlik Başkanlığı Hakkında 177 sayılı Cumhurbaşkanlığı Kararnamesi. Resmî Gazete (8 Ocak 2025).

Cumhurbaşkanlığı. (2025b). 192 sayılı Cumhurbaşkanlığı Kararnamesi (teşkilat yapısına ilişkin değişiklik). Resmî Gazete (25 Aralık 2025).

Ekimdzhiev ve diğerleri / Bulgaristan, B. No. 70078/12, AİHM (11 Ocak 2022).

Forseti Hukuk Bürosu. (2025). Siber Güvenlik Kanunu: 9 ay sonra neredeyiz? Kurumsal yapılanma, şirket yükümlülükleri ve gözden kaçan riskler. https://www.forseti.com.tr/genel/siber-guvenlik-kanunu/

Pekin Bayar Mizrahi. (2026a). Siber Güvenlik Başkanlığının yetki alanını genişleten kanun teklifi TBMM'ye sunuldu. https://pekin.com.tr

Pekin Bayar Mizrahi. (2026b). 7590 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun yürürlüğe girdi. https://pekin.com.tr

ProCompliance. (2026). Siber Güvenlik Başkanlığı'nın yetkileri genişliyor: Kanun teklifi neler öngörüyor? https://www.procompliance.net

Roman Zakharov / Rusya [BD], B. No. 47143/06, AİHM (4 Aralık 2015).

Szabó ve Vissy / Macaristan, B. No. 37138/14, AİHM (12 Ocak 2016).

Vladimir Kharitonov / Rusya, B. No. 10795/14, AİHM (23 Haziran 2020).

Weber ve Saravia / Almanya (k.k.), B. No. 54934/00, AİHM (29 Haziran 2006).

2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu. (1983). Resmî Gazete (3 Kasım 1983, S. 18210).

5237 sayılı Türk Ceza Kanunu. (2004). Resmî Gazete (12 Ekim 2004, S. 25611).

5271 sayılı Ceza Muhakemesi Kanunu. (2004). Resmî Gazete (17 Aralık 2004, S. 25673).

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. (2007). Resmî Gazete (23 Mayıs 2007, S. 26530).

burakolgun.com

5809 sayılı Elektronik Haberleşme Kanunu. (2008). Resmî Gazete (10 Kasım 2008, S. 27050).

6698 sayılı Kişisel Verilerin Korunması Kanunu. (2016). Resmî Gazete (7 Nisan 2016, S. 29677).

7545 sayılı Siber Güvenlik Kanunu. (2025). Resmî Gazete (19 Mart 2025, S. 32846). https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm

7590 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun. (2026). Resmî Gazete (31 Temmuz 2026, S. 33326).

burakolgun.com