

**Çevrimiçi Hizmetler ve İnternet İçerikleri Üzerindeki Yetki İcrasında Devletlerce
Başvurulan Yöntemlerin Uluslararası Hukuk Bağlamında Değerlendirilmesi****

*Evaluation of the Methods Applied by States in the Exercise of Jurisdiction over Online
Services and Internet Content in the Context of International Law*

Arş. Gör. Dr. Alp Eren TANYERİ***

Öz

İnternetin sınır aşan ve adem-i merkeziyetçi yapısı, geleneksel egemenlik anlayışına meydan okuyan hukuki ve teknik sorunlar doğurmuş; devletler, egemenlik kaynaklı yetkilerini kullanabilmek adına zamanla birtakım yöntemler geliştirmiştir. Eldeki çalışmada, söz konusu yöntemler fiili etkileri, dayandıkları ulusal hukuk düzenlemeleri ve uluslararası hukukun ilgili normları bağlamında incelenmiştir. Devletlerin internet üzerindeki yetki kullanımına ilişkin benimsedikleri farklı yaklaşımlar ABD, Çin, Rusya ve Türkiye örnekleri üzerinden mukayeseli olarak değerlendirilmiştir.

* **Makalenin Geliş Tarihi/Received:** 10.02.2025, **Makalenin Kabul Tarihi/Accepted:** 20.02.2025.

İntihal/Plagiarism: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir./This article has been scanned via a plagiarism software and reviewed by at least two referees.

** Bu çalışma, “Uluslararası Hukukta Devlet Egemenliğinin Bir Konusu Olarak Siber Uzay” başlıklı doktora tezinden türetilmiştir.

*** Tokat Gaziosmanpaşa Üniversitesi Hukuk Fakültesi Milletlerarası Hukuk Anabilim Dalı Araştırma Görevlisi (e-posta/e-mail: alperen.tanyeri@gop.edu.tr, ORCID: 0000-0003-1043-6011).

Gözetim ve denetim, içerik kaldırma, filtreleme ve erişim engelleme yöntemleri, sınır aşan etkileriyle egemenlik ihlalini gündeme getirebilmekte, insan hak ve özgürlükleri açısından da tartışmalara yol açmaktadır. Diğer taraftan, tüm önlemlere rağmen internette hukuka aykırılığın önüne yeteri kadar geçilemediği görülmektedir. Dolayısıyla devletlerin internet ortamındaki hukuka aykırılıklarla mücadele yolunda ulusal düzenlemelerine ve teknik kapasitelerine dayandığı; ancak gerçek anlamda etkili sonuçların elde edilebilmesi için uluslararası iş birliğine duyulan ihtiyacın arttığı tespit edilmiştir. Son olarak, ulusal hukuk mekanizmalarının ve uluslararası hukukun mevcut yapısının, internetin küresel etkisine cevap vermekte yetersiz kaldığına ve yeni uluslararası mekanizmaların geliştirilmesi gerekliliğine işaret edilmiştir.

Anahtar Kelimeler: İnternet, egemenlik, gözetim, içerik kaldırma, erişim engeli.

Abstract

The cross-border and decentralized structure of the internet has created legal and technical problems that challenge the traditional understanding of sovereignty, and states have developed various methods over time in order to exercise their sovereign jurisdictions. In the present study, these methods are analyzed in terms of their actual effects, the national legal regulations on which they are based, and the relevant norms of international law. The various approaches adopted by states in the exercise of jurisdiction over the Internet examined through a comparative approach using the examples of the United States, China, Russia and Türkiye.

Surveillance and control, content removal, filtering and access blocking methods can lead to violations of sovereignty due to their cross-border effects and also spark debates regarding human rights and freedoms. On the other hand, despite all measures, it is observed that illegality on the internet has not been sufficiently prevented. Therefore, it has been observed that states rely on their national regulations and technical capacities in the fight against illegal activities on the internet; however, international cooperation has become increasingly essential to achieving truly effective results. Finally, it has been highlighted that the current structure of national legal mechanisms and international law is inadequate to address the global impact of the Internet and that new international mechanisms need to be developed.

Keywords: Internet, sovereignty, surveillance, content removal, access blocking.

GİRİŞ

Dağıtık bir iletişim protokolü olarak ortaya çıkan internet, zamanla bütün küreye yayılarak bireysel ve kurumsal etkileşimleri yeniden yapılandırmış, hukuk sahasında yeni meselelere kapı açmıştır. Elektriğin uygun biçimde kullanımıyla fiziksel ve mantıksal unsurları bütünleştiren, bilginin aktarımında yer ve zaman etkisini asgari seviyeye indiren teknolojinin, fiziksel sınırlarla tanımlanan egemenlik öğretisine tesiri de kaçınılmaz olmuştur. Devletlerin egemenlik kaynaklı yetkilerini kullanma biçimleri, internetin sınır aşan adem-i merkeziyetçi doğasına uyarlanmak durumunda kalmıştır. Ortaya çıkan şartlar, uluslararası hukukun

geleneksel yetki kuramlarının internete tatbikinde yeni gerilim noktalarını beraberinde getirmiştir.

Devletler, internetin fiziksel ve mantıksal unsurları ile internette eylemde bulunan s jeler  zerinde hukuklarını tatbik edebilmek adına  e itli y ntemlere ba vurmaktadır. Fiziksel unsurlar ve s jeler, “ lke” ile nispeten daha sıkı ba lara sahiptir. Web siteleri, uygulamalar, veriler, internet trafi i vb. mantıksal unsurlar ise fiziksel altyapı  zerinde i lese dahi insan algısında sanal bir mek nın tecr be edilen kısımları olarak kar ılık bulmaktadır. Ancak bu unsurlar, devletin  lkesinde do rudan etki do urabilmekte ve  lkeden ba ımsız olarak vatandaşlarla etkile imine imk n sa layabilmektedir. Hukuk disiplini altında verinin, ba lı başına kapsamlı, detaylı ve  zg n nitelikleri olan bir unsur olarak farklı  alı malarda ayrıca incelenmesi gereklidir. İnternet olgusuyla birlikte ilk akla gelen  evrimi i hizmetler ve internet i erikleri ise eldeki  alı manın temel unsurları olarak belirlenmi tir. Devletlerin s z konusu unsurlar  zerindeki yetki icrasında ba vurdukları y ntemler de “g zetim ve denetim”, “i erik kaldırma”, “filtreleme ve eri im engelleme” şeklinde    ana ba lık altında ele alınmı tır. Nitekim sahip olunan imkanlar nispetince kullanılabilecek sayısız teknik ve ara metot, bu ana ba lıkların altında yer almaktadır.

A a ıda de erlendirilen y ntemler insan hakları, etkililik ve uluslararası hukuka uygunluk bakımından tartı maya a ık ve helere sahiptir. Nasıl ki internet ortamında sunulan hizmet ve i erikler, d nyanın hemen her yerinde eri ilebilir olmasından m tevellit etki do uruyorsa; s z konusu unsurlara y nelik devletlerce ba vurulan y ntemler de yer yer  lke dı ında etki do urabilmektedir.  lke i inde de milli g venlik, kamu d zeni ve insan hakları arasındaki denge arayı ında yeni zorluklarla kar ıla ılmaktadır. T m hukuki sorunların   z ld   bir ihtimalde dahi y ntemlerin amaca uygunlu u ve etkilili i a ısından devletlerin ulusal kapasitelerini a an sorunlar g ndeme gelmektedir.

Eldeki  alı mada, yukarıda bahsi ge en y ntemler; dayandıkları ulusal hukuk d zenlemeleri, uluslararası hukukta devletin yetkisine h kim ilkelere uygunlukları ve etkililikleri ba lamında de erlendirilmi tir. Kapsamlı bir uluslararası antla manın ve k kle mi  uluslararası  rf ve  det hukuku kurallarının yoklu unda devlet uygulamaları, uluslararası hukuk a ısından ziyadesiyle  nem kazanmaktadır. Bu do rultuda, internet  zerindeki etkinlik seviyeleri ve izledikleri internet politikalarındaki  e itlilik dikkate alınarak ABD,  in, Rusya ve T rkiye  rnekleri  alı ma kapsamına dahil edilmi tir. İnternetin k resel yapısının, egemenlik kaynaklı yetkilerin kullanımına etkisi tartı ılmı ; devletlerin mevzubahis sahadaki yetki icrasında kar ıla tıkları hukuki ve teknik sorunlara dikkat  ekilmi tir. Devlet egemenli inin internet ortamına n fuzunun uluslararası hukuk  er evesinde sa lanabilmesi adına, uluslararası i  birli i mekanizmalarının g  lendirilmesine duyulan ihtiya  vurgulanmı tır.

I. İNTERNET, WEB,  EVİRİMİ İ HİZMETLER VE İNTERNET İ ERİKLERİ

İleti im, haberle me ve y netim s re lerine hizmet eden tekniklerin temel prensipleri, teknoloji ilerledik e bi im ve y ntem olarak de i se de  z nde bilgi payla ımı ve

organizasyonunun kadim esaslarına dayanır. İnternetin kök bulduğu zemin, sözgelimi Bizans'ın 9. yy'da Müslüman akınlarına karşı Hasan Dağı'ndan İstanbul'a kadar belirli aralıklarla ateşli sinyal kuleleri inşa ederek kurduğu, haberlerin 720 km gibi bir mesafeyi bir saat içinde kat etmesini sağlayan sistem¹ ile ortaktır. Öyle ki; 19. yy'ın hemen başında, İngiltere'nin Devon Kontluğu'nda, aynı sitemle şehri bir ağ gibi sararak günümüz ağ haritalarına benzeyen bir işleyiş meydana getirildiği de görülmektedir.² Atlı habercilerden posta teşkilatlarına ve telgraftan uydu sistemlerine kadar iletişimin uzun tarihi, ortak bir öze ilişkin çabaların sonucudur. Dolayısıyla internetin söz konusu araçsal geleneğin bir parçası olduğunu ilk kertede kabul etmek gerekir.

İnternetin benzer kavramlardan ayırt edilmesi, devlet ve hukuk ile ilişkilendirilmesinde yapılacak çözümlemelerin sarahat ve isabeti adına önem arz etmektedir. Eldeki çalışmanın kapsamının tespiti bakımından ise ortaya çıkış şartları bağlamında internet ve Web ilişkisini açıklayarak, internetin sahip olduğu fiziksel (*physical*) ve mantıksal (*logical*) yapıların ayrımının vurgulanması faydalı olacaktır.

Soğuk Savaş atmosferindeki 1958 yılında Amerika Birleşik Devletleri (ABD) Savunma Bakanlığı tarafından “İleri Araştırma Projeleri Ajansı (*Advanced Research Projects Agency-ARPA*)” kurulmuştur.³ 2. Dünya Savaşı'nda atom bombasının kullanılması trajik bir “teknolojik sürpriz” örneği olarak görülürken; *ARPA*'nın temel fonksiyonunun “ABD aleyhine teknolojik sürpriz yaşanmasını engellemek” olduğu, bunun da ancak “sürprizleri yapan taraf” olmakla mümkün olduğu değerlendirilmiştir.⁴ Nükleer savaş tehdidinin yükseldiği dönemlerde, olası nükleer saldırı durumunda emir komuta sisteminin işlevini devam ettirebilmesini sağlayacak bir iletişim sistemi ihtiyacı doğmuştur.⁵ Bu amaçla önerildiği üzere dağıtık ağların (*distributed network*) paket anahtarlama (*packet switching*) yöntemiyle çalışması prensibi⁶ uygulanan ve *ARPA* araştırmacılarının bilgisayarlar vasıtasıyla iletişim kurmalarını sağlamak amacıyla 1969'da faaliyete geçen *ARPANET* (*Advanced Research Projects Agency Network*), günümüzde internet olarak adlandırılan yapının temelini oluşturmuştur. 1983'te, *ARPANET*'in araştırma amaçlı kullanılan ağı aynı isimle devam ederken; askeri amaçlı ağ, *MILNET* (*Military Network*) adıyla ayrılmıştır. Ağda kullanılan Ağ Kontrol Protokolü'nden (*Network Control Protocol-NCP*) İletim Kontrol Protokolü / İnternet Protokolü'ne

¹ Philip Pattenden, ‘The Byzantine Early Warning System’ (1983) 53 *Byzantion* 258, 258–299.

² Devon County Council, ‘Fire Beacons: Warning Signals Across the Countryside’ (2000) 7 <<https://devoncc.sharepoint.com/sites/PublicDocs/Environment/Historic/Forms/AllItems.aspx?id=%2Fsites%2FPublicDocs%2FEnvironment%2FHistoric%2FSchools%2FFire%20Beacons%2Epdf&parent=%2Fsites%2FPublicDocs%2FEnvironment%2FHistoric%2FSchools&p=true&ga=1>> Erişim Tarihi: 05.02.2025.

³ US Department of Defence, ‘Department of Defense Advanced Research Projects Agency’ (Directive, No 5105.15, 7 February 1958).

⁴ Stephen Lukasik, ‘Why the Arpanet Was Built’ (2011) 33 *IEEE Annals of the History of Computing* 4, 6.

⁵ *ibid* 9.

⁶ Saldırı senaryolarına göre sistem alternatiflerinin verimliliğine yönelik analizler ve söz konusu prensip hakkında ayrıntılı bilgi için bkz Paul Baran, ‘On Distributed Communications Networks’ (The RAND Corporation 1962) R-2626.

(*Transmission Control Protocol / Internet Protocol-TCP/IP*) geçiş de bu yılda gerçekleşmiştir.⁷ 1989'da da amacını başarıyla gerçekleştirmiş olan *ARPANET* kapanmıştır.⁸ Bu süreç, ABD Ulusal Bilim Vakfı'nın (*National Science Foundation-NSF*) ülke çapındaki birçok üniversiteyi birbirine bağlama çalışmalarının sonucu olarak 1986'da *NSFNET*'i (*National Science Foundation Network*) faaliyete geçirmesiyle paralellik taşımaktadır.⁹ *NSFNET* ile internetin omurgası oluşmuş; koordinasyonu ise İnternet Tahsisli Sayılar ve İsimler Kurumu'nun (*Internet Corporation for Assigned Names and Numbers-ICANN*) 1998'de yetkilendirilerek özelleştirilmesine kadar devlet marifetiyle sürdürülmüştür.¹⁰

Yukarıda arz edilenlerden anlaşılacağı üzere “internet”; esas itibariyle iletişim ve veri paylaşımı amaçlı, belirli teknik standart ve kurallara göre kurulup işletilen bir dağıtık bağlantı sistemidir. Uygun cihazları, uygun fiziksel altyapıya bağlamak suretiyle internetin bir parçası olunmaktadır. Telefon ya da telgraf ağları da kendi standart ve kuralları dâhilinde farklı bağlantı sistemi örnekleri olarak gösterilebilir. İnterneti başka sistemlere göre çok ileri noktaya taşıyan ilk unsur ise şüphesiz ki bilgisayar ve dağıtık ağ bağlantı teknolojilerinin gelişimidir. Bu ileri seviye teknolojik altyapı da Web fikrine yaşam alanı sağlayarak “sanal alem” ifadesiyle karşılık bulan ortamı günümüze kadar taşımıştır.

1980'li yıllarda, Cenevre'de faaliyetlerini sürdüren Avrupa Nükleer Araştırma Merkezi (*Conseil Européen pour la Recherche Nucléaire-CERN*) bünyesinde belirli periyotlarla çalışıp ayrılan araştırmacıların ürettiği verilerin, toplanıp koordine edilerek, yeni araştırmacıların da faydalanabileceği şekilde birikimli hale getirilmesi amacıyla bir formül ihtiyacı doğmuştur.¹¹ *ARPANET* ve *NSFNET* dönemlerine tekabül eden bu süreçte internet, ortaya çıkış amacını karşılamış olsa da kullanımının uzmanlık gerektirmesi, altyapısının çok pahalı ve karmaşık olması, sınırlı amaçlar dışında verimli kullanılamaması gibi zaafları nedeniyle söz konusu ihtiyacı tam anlamıyla karşılayamamıştır.¹² O dönem içinde *CERN*'de görevli olan *Tim Berners-Lee*, 1989'da sunduğu “Bilgi Yönetimi: Bir Öneri” başlıklı çalışmada, dağıtık “hiper metin (*hypertext*)”¹³ sistemini temel alan bir çözüm öngörmüştür.¹⁴ Önerdiği sistem için

⁷ Ronda Hauben, ‘From the ARPANET to the Internet’ (23 Haziran 1998) <https://www.columbia.edu/~rh120/other/tcpdigest_paper.txt> Erişim Tarihi: 05.02.2025.

⁸ Lukasik (n 4) 17.

⁹ US National Science Foundation, ‘Birth of the Commercial Internet’ <<https://new.nsf.gov/impacts/internet>> Erişim Tarihi: 05.02.2025.

¹⁰ Susan Schiavetta and Konstantinos Komaitis, ‘ICANN’s Role in Controlling Information on the Internet’ (2003) 17 *International Review of Law, Computers & Technology* 267, 268–269.

¹¹ Tim Berners-Lee and Mark Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor* (1st ed, HarperSanFrancisco 1999) 3–23.

¹² ibid 18.

¹³ Hiper metinler, salt yazıdan ibaret olmanın ötesinde, medya içeriği, diğer metinlere bağlantılar vs. özellikleri de içerisinde barındırabilen belgelerdir. Günümüzdeki “web sayfası” kavramının temeli, bu belge yönteminin ortaya çıkışıyla atılmıştır. Ayrıntılı bilgi için bkz Roy Rada, ‘Writing and Reading Hypertext: An Overview’ (1989) 40 *Journal of the American Society for Information Science* 164.

¹⁴ Timothy J Berners-Lee, ‘Information Management: A Proposal’ (CERN 1989) <<https://cds.cern.ch/record/369245>> Erişim Tarihi: 05.02.2025.

de en uygun altyapı internettir. Bu sayede dünyanın çeşitli yerlerinde bulunan kullanıcıların internet üzerinden aynı bilgilere farklı bilgisayar sistemleriyle ulaşmaları ve bilgilerin bulunduğu hiper metinlere kendi özel bağlantılarını (*link*) eklemeleri sağlanmış; ayrıca daimî değişkenlik arz eden bilgilere eş zamanlı erişmeyi sağlayan “canlı” bağlantıların kurulması mümkün hale gelmiştir.¹⁵ Önerinin 1990’da kabulünü izleyen süreçte işlemeye başlayan sisteme ise “Dünya Çapında Ağ (*World Wide Web-WWW*)”¹⁶ adı verilmiştir.¹⁷

Paket anahtarlama mantığı gereği, ileti transferinde paketin bir cihazdan başkasına ulaşabilmesi için internete bağlı her cihazın bir IP adresine sahip olması gereklidir. Dolayısıyla bir Web sitesine erişmek istendiğinde, siteyi barındıran cihazın (sunucunun-*server*) adresine ihtiyaç duyulmaktadır. Bu adreslerin de bilinirliğinin sağlanması ve kullanıcı dostu olması amacıyla çok sayıda rakamdan¹⁸ oluşmuş karmaşık *IP* adresleri yerine; bu IP adresleriyle eşleştirilen “www.example.com” gibi alan adları tercih edilmiştir. Alan Adı Sistemi (*Domain Name System-DNS*) de özet olarak, bu unsurların ve eşleştirmelerin dağıtık şekilde tutulduğu bir veri tabanını ifade etmektedir.¹⁹

Web sayesinde metin ve medya öğelerini barındıran sayfalar, yine barındırdıkları linklerle birbirine bağlanmış ve böylece internetin sağladığı fiziksel ağın üzerinde “yaşayan” bir soyut ağ meydana getirmiştir. Web sayfalarının hiper metin ile sahip olduğu bu özellikler sebebiyle, Web’in ilk yıllarından itibaren birçok yazar bu sistemi sanal bir uzay metaforu kullanarak tanımlamıştır.²⁰ Türkçeye “sanal alem” tabiriyle yerleşen söz konusu metafor, esasında internetin Web ve içerikleri ile popülerleşen mantıksal yapısının insan algısındaki izdüşümünü ifade etmektedir. Sonuç itibarıyla dar anlamda internet, belirli standartlar ve protokoller çerçevesinde oluşturulmuş, fiziksel araçlarla birbirine bağlanan bir ağlar ağıyken; geniş anlamda ise internetin cihazlar, kablolar ve çeşitli bağlantı elemanları gibi fiziksel unsurlarla birlikte Web’i ve diğer mantıksal unsurları, üzerinde iletimini sağladığı verileri ve ağa bağlanan kişileri de kapsayan geniş bir sistem olarak tanımlanması mümkündür. Çevrimiçi hizmetler de internetin mantıksal yapısına dahil olan başta Web siteleri ve uygulamalar olmak üzere, internete bağlı kalma şartıyla kullanılabilen hizmetleri ifade etmektedir.

İnternet bağlamında “içerik” ise hukuken oldukça kapsamlı bir ifadedir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun²¹ metninde tercih edilen “*internet ortamı üzerinden*

¹⁵ Tony Kippenberger, ‘How Did We Get to a World Wide Web?’ (1999) 4 The Antidote 21, 22.

¹⁶ Eldeki çalışmanın devamında “Web” kısaltmasıyla ifade edilecektir.

¹⁷ Berners-Lee and Fischetti (n 11) 23.

¹⁸ IPv4’ün 32 bitlik sisteminde adresler 93.184.215.14 gibi rakamlardan oluşurken; 128 bitlik gelişmiş versiyon IPv6 sistemine göre alınan adresler 2606:2800:21f:cb07:6820:80da:af6b:8b2c gibi harf ve rakam kombinasyonlarından oluşabilmektedir.

¹⁹ Milton L Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (1. paperback ed, MIT Press 2004) 41.

²⁰ Rainer Bromme and Elmar Stahl, ‘Is a Hypertext a Book or a Space? The Impact of Different Introductory Metaphors on Hypertext Construction’ (2005) 44 Computers & Education 115, 117.

²¹ 04.05.2007 tarih ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (RG 23.5.2007/26530).

*kullanıcılara sunulan her türlü bilgi veya veri...*²² tanımı da bunun bir göstergesidir. İçeriğin, Avrupa Birliği (AB) Dijital Hizmetler Yasası (*Digital Services Act-DSA*)²³ düzenlemesinde “yasadışı içerik (*illegal content*)” başlığında “...herhangi bir bilgi”;²⁴ ABD’de telekomünikasyona dair federal yasaları kodifiye eden 47 U.S. Code hükümlerinde, “bilgi içeriği sağlayıcı (*information content provider*)” başlığında “...internet veya diğer etkileşimli bilgisayar hizmetleri aracılığıyla sağlanan bilgi...”;²⁵ Birleşik Krallık Çevrimiçi Güvenlik Yasası (*Online Safety Act*) hükümlerinde ise “...bir internet hizmeti aracılığıyla iletilen herhangi bir şey...”²⁶ şeklinde tanımlandığı görülmektedir. Dolayısıyla içeriği belli türlerle sınırlı sayıya tabi tutmak mümkün değildir. Dijital ortama taşınmış her veri, hukuken “içerik” kapsamındadır. Dijital formdaki içerik de internet vasıtasıyla erişilebilir olduğu durumda “internet içeriği” vasfını haiz olacaktır.

Sonuç olarak, eldeki çalışmada internet geniş anlamıyla değerlendirilmiş; devletlerin yetki icrasında başvurdukları yöntemler ile uluslararası hukukta egemenlik ve yetkiye ilişkin esaslar bakımından, başta Web siteleri ile dijital platformlar olmak üzere çevrimiçi hizmetler ve genel olarak internet içerikleri kapsam dahiline alınmıştır. İnternetin fiziksel yapısı, internette eylemde bulunan sükeler ve internet erişimine açık kişisel veriler ile büyük veri (*big data*) gibi unsurların devletler ile münasebeti de farklı çalışmalara konu edilebilir.

II. ÇEVİRİMİÇİ HİZMETLER VE İNTERNET İÇERİKLERİ ÜZERİNDEKİ YETKİ İCRASINDA DEVLETLERCE BAŞVURULAN YÖNTEMLER

Devletler, uluslararası hukukun devletin yetkisine hâkim ilkelerine²⁷ binaen internetin fiziksel altyapısı ve internette eylemde bulunan sükeler üzerinde yetkili olduğu gibi, internetin mantıksal yapısı üzerinde de yetki sahibidir. Özellikle Web mimarisinin sonucu olarak; devletlerin mantıksal unsurlara ve verilere müdahalesi, yabancı veya ülke dışındaki kişiler

²² 5651 sayılı Kanun, m 2/1-f.

²³ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.

²⁴ Digital Services Act, art 3/h.

²⁵ Communications Decency Act, 47 USC § 230 (1996).

²⁶ Online Safety Act 2023, c 50, s 236(1).

²⁷ Bir siyasal iktidar tipi olarak devletin en temel hukuki fonksiyonları, kural koymak ve tatbik etmektir. Hangi olgular hakkında kural konabileceği ve kuralların bu olgulardan hangilerine, hangi şartlarda tatbik edilebileceği, yine devletlerin zaman içinde uluslararası hukuk nezdinde ortaya koyduğu esaslara göre belirlenmektedir. Söz konusu esaslar, devlet otoritesinin ülke ve insan üzerinde sahip olduğu siyasal iktidarından doğan “yer yönünden (*ratione loci*)” ve “kişi yönünden (*ratione personae*)” yetkisini (*jurisdiction*) yansıtabilecek şekilde, başta vatandaşlık ve ülkesellik bağlarına dayanmaktadır. Mezkûr bağların doğrudan kurulamadığı durumlarda dahi devletin bizzat kendisini veya vatandaşlarını koruması yahut evrensel kabul görmüş suçlarla mücadele edilebilmesi adına yetkinin varlığından bahsedilebilmektedir. Bu mülâhazalar ile ortaya çıkan ilkelere dair sistematik bilgi için bkz Rebecca MM Wallace and Olga Martin-Ortega, *International Law* (8th edn, Sweet & Maxwell 2016) 124–142; Martin Dixon, *Textbook on International Law* (7th edn, Oxford University Press 2013) 148–161; Malcolm N Shaw, *International Law* (8th edn, Cambridge University Press 2017) 483–522; Christopher Staker, ‘Jurisdiction’ in Malcolm D Evans (ed), *International Law* (4th edn, Oxford University Press 2014) 309–333; Tim Hillier, *Principles of Public International Law* (2nd edn, Cavendish Publishing 1999) 125–141.

üzerinde yetki tespit ve icrasına göre çoğu kez daha rahat şekilde gerçekleşmektedir. İnternet içeriğine devlet müdahalesi, resmî kurumlar vasıtasıyla doğrudan icra edilebileceği gibi başta erişim sağlayıcılar (yaygın kullanılan tabirle İnternet Servis Sağlayıcılar-İSS) olmak üzere hizmet sağlayıcılar vasıtasıyla da meydana gelebilmektedir.

Muhtelif amaçlarla belli kullanıcılar arasında kapalı devre iletişim olanağı sağlayan intranet sistemleri dahi ülke veya uyruklu ilişki kurulabildiği yahut buralardan kaynaklanan etkilere maruz kalındığı takdirde devlet yetkisine tabidir. Mezkûr sistemlerin sözcüğü bir soruşturma kapsamında gizli takibe alınması yahut açıktan ve cebren müdahale etmek suretiyle erişim sağlanması gibi uygulamalar, hukuken öngörölmüş şartlar karşılandığında devletler için mümkündür. İnternette ise *TOR (The Onion Router) Ağı*²⁸ gibi alternatif ağların yahut IP üzerinden Ses İletimi (*Voice over Internet Protocol-VoIP*), Dosya Aktarım Protokolü (*File Transfer Protocol-FTP*), İnternet Aktarmalı Sohbet (*Internet Relay Chat-IRC*) gibi uçtan uca (*peer to peer-P2P*) protokollerin kullanımında da benzer durum geçerlidir. Web ise hiper metin ve hiper link yapısı, kamusallaşması ve İSS'ler ile site işletmecilerinin tahakkümünde olması yönüyle farklılaşmaktadır. Ortaya çıktığı zamanlardaki adem-i merkezîyetçi yapısıyla özgürlük ve devletlerden bağımsızlık rüzgarına sebep olan Web, günümüzde ana hatlarıyla oldukça kontrol edilebilir hale getirilmiştir. Devletler için sùjeler ve fiilleri üzerindeki yetki icrasının yanında, Web içerikleri üzerindeki icra imkanları da gelişmiştir. Genellikle İSS'ler, yer sağlayıcılar ve Web sitesi işletmecilerini muhatap alan devletler,²⁹ Web içeriklerine yapılacak müdahaleleri bu muhatapları vasıtasıyla gerçekleştirmektedir. Söz konusu içerikler için; gözetleme ve denetleme, kaldırma, filtreleme ve erişim engelleme gibi yöntemlere başvurulabilmektedir.

A. Gözetim ve Denetim

Devletlerin, ülkelerinde meydana gelen olaylar ve kişilerin eylemleri üzerinde gözetim ve denetim yetkisine sahip olması, devlet olmanın doğal bir sonucudur. Lakin bu yetkinin sınırlarına dair tartışmalar muhtemeldir ki devlet mefhumu var olduğu sürece devam edecektir. Mamafih kamu düzeni ve milli güvenlik gibi kaygılar ile insan hak ve özgürlükleri arasındaki dengeyi sağlamak, hukukun çetin bir vazifesidir. Devletlerin ulusal hukuk düzenlemelerinin ve

²⁸ TOR ağının işleyişine dair bkz Merve Varol Arısoy and Ecir Uğur Küçüksille, 'Performance Comparison of TOR Hidden Service Crawlers' (2019) 6 Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi 147, 149–151.

²⁹ Söz konusu sùjeler, literatürde sıklıkla "hizmet (veya servis) sağlayıcı" kümesi içinde anılmaktadır. Geniş anlamıyla ele alındığında, her birinin esasen internet işleyişi dahilinde birer hizmet sağlıyor olmasından bahisle hizmet sağlayıcı olarak anılması mümkündür. Fakat bu yöntem, küme içinde ayırım yapılırken bazı karışıklıklara sebep olmaktadır. Örnek olarak "internet servis sağlayıcı", erişim sağlayıcıyı, yer sağlayıcıyı ve Web sitesi işletmecisini belirtecek şekilde kullanılabilir. Oysa yerleşik kullanımda İSS (veya İngilizce'den ISP) kısaltması, esasen abonelerine internet hizmeti sunan operatörleri, yani erişim sağlayıcı ifade etmektedir. Öztekin de bu durumu, İSS kavramının bir çatı kavram olarak kullanılmasıyla dar manada kullanılması arasındaki fark ile açıklamıştır; Alp Öztekin, *Teori ve Uygulamada Türk İnternet Hukuku* (1. bs, Seçkin Yayıncılık 2021) 156. Eldeki çalışmada da erişim sağlayıcılar "İSS"; çevrimiçi hizmetlere ve internet içeriklerine barındırma (*hosting*) hizmeti sunan sùjeler "yer sağlayıcı"; içeriğini kendisi sağlayan veya içerik sağlayıcıların içeriklerini internet ortamında erişilebilir kılması için aracılık hizmeti veren çevrimiçi uygulama veya Web sitelerini işletenler de "Web sitesi işletmecisi" sıfatıyla karşılanmıştır.

mer’i uygulamalarının bu bakımdan yerindeliği meselesi, anayasa ve insan hakları çerçevesinde farklı çalışmaların konusudur. Modern egemen devletler sistemine dayalı uluslararası hukukun konu hakkındaki esas meselesi ise; yetki doktrinleriyle tesis ve icra sınırları belirlenen devletlerin, sınır aşan ve bütünü üstünde egemenlik iddiası mümkün olmayan internet üzerindeki gözetim ve denetim normları ve uygulamalarınca oluşan vakıanın tespiti. Zira devletleri bundan meneden yahut açıkça sınırları belirleyen bir uluslararası hukuk kaynağının yokluğunda, devlet normları ve uygulamaları rehber niteliğinde kabul edilecektir.

İnternet bağlamında “gözetim (*surveillance*)”³⁰ eylemi, en sade tanımla kullanıcılar ile sunucular arasındaki trafiğin ve içeriğin takibini ifade etmektedir. Web’in geçirdiği evrim ve kullanıcıların internet ortamına sağladığı içeriğin ulaştığı çeşitlilik ile büyüklük, gözetimi sosyal ve siyasal açıdan çok kapsamlı ve etkili bir araç haline getirmiştir. İnternet gözetimi, teknoloji temelli bir eylem olduğundan, öncelikle teknoloji sahiplerinin fiilen elinde bulundurduğu bir imkândır. Dolayısıyla akla ilk olarak şirketler gelmektedir. İnternet hizmetlerini doğrudan kullanıcıyla buluşturan şirketler, hizmetlerin kullanımıyla ortaya çıkan veri yığınına karşı hâkim pozisyonundadır. Devletlerin de hem doğrudan teknoloji kullanımı marifetiyle hem şirketler üzerindeki otoritesini kullanmak suretiyle gözetim icra etmesi mümkündür. Gerek şirketler gerek devletler tarafından yürütülen gözetim açık veya örtülü, hukuki veya hukuka aykırı olabilir. Şirketlerin önceliği genellikle reklam isabeti, kullanıcı alışkanlıklarının tespiti, pazar hakimiyeti, verilerden maddi menfaat sağlanması gibi ekonomik/ticari motivasyonlardır. Devletler ise kamu düzeninin ve milli güvenliğinin temini başlığı altında; siber güvenlik, terörle mücadele, suçun tespiti ve önlenmesi, kitlelerin siyaseten kontrolü veya baskı altına alınması, mali denetim, hak ve özgürlüklerin muhafazası, dezavantajlı grupların korunması gibi hukuki veya siyasi amaçlar taşıyabilir. Devletlerin gözetim ve denetim faaliyetleri amaç ve süre itibarıyla sınırlı tutulabilir ya da sürekli ve genel uygulamalara başvurulabilir. Devletler ve şirketler dışında uluslararası örgütler, sivil toplum kuruluşları ve gönüllüler tarafından, çocuk istismarı gibi kamu vicdanında büyük tahribata sebep olan suçlara karşı düzenli izleme, raporlama ve bildirim faaliyetleri de yürütülmektedir.³¹

³⁰ Literatürde bilgi ve iletişim teknolojilerinin kullanımı yoluyla gözetim/izleme için “veri gözetimi/verizleme (*dataveillance*)”, dijital/elektronik gözetim, elektronik panoptikon gibi kullanımlar tercih edilmektedir; Christian Fuchs and others, ‘Introduction: Internet and Surveillance’ in Christian Fuchs and others (eds), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (1st edn, Routledge 2012) 1; Taha Kurt, ‘Panoptikondan Data Diktatörlüğüne: Özgürlüğün Sonu mu?’ (2023) 1 Tokat Gaziosmanpaşa Üniversitesi Hukuk Fakültesi Dergisi 137, 142–144.

³¹ Uluslararası Kriminal Polis Teşkilatı (*The International Criminal Police Organization-INTERPOL*) bünyesindeki Çocukların Cinsel İstismarı Uluslararası Veri Tabanı (*International Child Sexual Exploitation (ICSE) Database*), Uluslararası İnternet İhbar Merkezleri Birliği (*International Association of Internet Hotlines-INHOPE*), İnternet İzleme Vakfı (*Internet Watch Foundation-IWF*), gibi kurumlar örnek olarak gösterilebilir. Haklarında detaylı bilgi için bkz ‘International Child Sexual Exploitation Database’, (*INTERPOL*) <<https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database>> Erişim Tarihi: 05.02.2025; ‘Association of Internet Hotline Providers’, (*INHOPE*) <<https://www.inhope.org/EN>> Erişim Tarihi: 05.02.2025; ‘About Us’, (*IWF*) <<https://www.iwf.org.uk/about-us/>> Erişim Tarihi 05.02.2025.

Uluslararası hukukta internet gözetimine dair sınırlar, insan hakları sözleşmelerinden başlamaktadır. İnsan Hakları Evrensel Beyannamesi,³² Medeni ve Siyasi Haklar Sözleşmesi,³³ Avrupa İnsan Hakları Sözleşmesi (AİHS)³⁴ gibi metinlerde özel hayatın ve haberleşmenin mahremiyeti vurgulanmıştır. Bilişim özelinde ise BM Genel Kurulu, 2014 tarihli “Dijital Çağda Mahremiyet Hakkı” başlıklı kararıyla devletlere şu çağrılarda bulunmuştur:³⁵

“(a) Dijital iletişim bağlamı da dahil olmak üzere mahremiyet hakkına saygı gösterilmesi ve onun korunması;

(b) İlgili ulusal mevzuatın uluslararası insan hakları hukuku kapsamındaki yükümlülüklerine uygunluğunu temin etmek de dahil olmak üzere, bu hakların ihlallerine son vermek ve bu tür ihlalleri önleyecek şartları sağlamak için tedbirler almak;

(c) Uluslararası insan hakları hukuku kapsamındaki tüm yükümlülüklerinin tam ve etkili bir şekilde uygulanmasını sağlayarak mahremiyet hakkını idame ettirmek amacıyla; kitlesel gözetim, dinleme ve toplama dahil olmak üzere iletişimlerin gözetimi, dinlenmesi ve kişisel verilerin toplanmasıyla ilgili usullerini, uygulamalarını ve mevzuatlarını gözden geçirmek;

(d) İletişimlerin devletçe gözetimi, dinlenmesi ve kişisel verilerin toplanması için uygun ölçüde şeffaflığı ve hesap verilebilirliği sağlayabilecek bağımsız, etkili yerel denetim mekanizmaları kurmak veya mevcut olanları sürdürmek”

İnsan hak ve özgürlüklerine ilişkin sınırlar, uluslararası hukukun temelini oluşturan devlet egemenliğine dayalı iktidara karşı çizilmiştir. Diğer taraftan devletlerin egemen eşitliği ve iç işlerine karışmama ilkeleri de küresel kabul görmüş durumdadır. Bu bakımdan devletin internet üzerindeki iç egemenliğine tekabül eden yetkisinin ilk basamağı gözetim ve denetim olacaktır.

İnternet üzerinde etkin gözetim politikaları izleyen Çin, Siber Güvenlik Yasası³⁶ hükümleriyle vatandaşlarına güvenli ve yaygın şekilde ağ erişimi sunmayı taahhüt etmiş; ağları kullanan vatandaşların da rejime ve sosyoekonomik düzene tehdit teşkil edecek davranışlarda

³² İnsan Hakları Evrensel Beyannamesi, m 12: “Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır.”

³³ Medeni ve Siyasi Haklar Sözleşmesi, m 17: “Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bulunulamaz.”

³⁴ AİHS, m 8: “1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”

³⁵ UN General Assembly Resolution 68/167, The Right to Privacy in the Digital Age, UN Doc A/RES/68/167, (18.12.2013), 2-3.

³⁶ Yasanın İngilizce çevirisi için bkz ‘Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017)’ (DigiChina) <<https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>> Erişim Tarihi: 05.02.2025.

bulunmalarını yasaklamıştır.³⁷ Ayrıca hukuka uygunluğun denetimi ve tehditlere karşı güvenliğin sağlanması için de bir “siber güvenlik izleme, erken uyarı ve bilgi iletişim sistemi” kurulmasına hükmedilmiştir.³⁸ Çin ayrıca her devletin sınırları içerisindeki veri akışını tamamen kontrol etme yetkisi olduğunu kabul etmektedir.³⁹ Çin’de düzenleme, gözetim ve denetim yetkileri Çin Siber Uzay İdaresi, Kamu Güvenliği Bakanlığı, Endüstri ve Bilgi Teknolojileri Bakanlığı ve Devlet Piyasa Düzenleme İdaresi olmak üzere dört merkezi kuruma tanınmış durumdadır. Lakin esas olarak genel veri akışı üzerindeki gözetim ve denetim işlevleri Çin Siber Uzay İdaresi tarafından yerine getirilmektedir.⁴⁰ Bunların yanı sıra hizmet sağlayıcılara da platformlarındaki bilgi yönetimlerini güçlendirmeleri, böylece tespit ettikleri hukuka aykırı içerikler hakkında, yayılmasını engelleme, yetkili makamlara bildirme, silme gibi önlemleri uygulamaları yükümlülüğü getirilmiştir.⁴¹

ABD’nin 11 Eylül sonrasındaki güvenlikçi politikalarının sembollerinden olan ABD Yurtseverlik Yasası’nın (*USA PATRIOT Act*)⁴² 215. Bölüm hükümleri ile devlete internet üzerinde geniş bir gözetim yetkisi tanınmıştır.⁴³ Yasanın süresi 2015’te dolduğunda ise bu kez ABD Özgürlük Yasası (*USA FREEDOM Act*)⁴⁴ adında yeni bir yasa ile reforma gidilmiştir. Aradaki süreçte 1978 tarihli Yabancı İstihbarat Gözetimi Yasası’nda (*Foreign Intelligence Surveillance Act-FISA*) reform yapılmış ve 2008 tarihli *FISA* Değişiklikleri (*FISA Amendments*)⁴⁵ kabul edilmiştir. Sonuçta ABD hukukunda internet gözetimine dair hukuki dayanak, Yurtseverlik Yasası ile getirilen normların Özgürlük Yasası ile tadil edilmiş halinden ve *FISA* normları tarafından tamamlanmış kısımlardan müteşekkildir.⁴⁶ *FISA* hükümleriyle ABD hükümetine, ABD dışındaki kişilerin internet hareketlerinin milli güvenlik gerekçesiyle gözetimi için yetki tanınmıştır. Gelgelelim bu yetkinin Ulusal Güvenlik Ajansı (*National Security Agency-NSA*) tarafından ABD ülkesindeki ABD vatandaşlarının bilgileri için de kullanılmak suretiyle istismar edildiği, işleyişi gizlilik esasına göre yürüyen *FISA*

³⁷ Çin Siber Güvenlik Yasası, m 12.

³⁸ Çin Siber Güvenlik Yasası, m 51.

³⁹ Cemre Çise Kadioğlu Kumtepe, ‘Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliğinin Tallinn Rehberi Kapsamında Değerlendirilmesi’ (2022) 53 *The Turkish Yearbook of International Relations* 21, 26.

⁴⁰ Angela Huyue Zhang, *High Wire: How China Regulates Big Tech and Governs Its Economy* (Oxford University Press 2024) 142–143.

⁴¹ Çin Siber Güvenlik Yasası, m.47.

⁴² Yasanın resmi ve tam adı: “*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*”.

⁴³ ‘Surveillance Under the USA/PATRIOT Act’ (*American Civil Liberties Union*) <<https://www.aclu.org/documents/surveillance-under-usapatriot-act>> Erişim Tarihi: 05.02.2025.

⁴⁴ Yurtseverlik yasasına benzer şekilde yasanın resmi ve tam isimden anlamlı bir kısaltma çıkarılmıştır: “*Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*”.

⁴⁵ Public Law No 114-23, 129 Stat 268 (2 Haziran 2015).

⁴⁶ 215. Bölüm özelinde düzenlemeler arasındaki ilişkiye dair resmi bilgilendirme için bkz ‘USA Freedom Act’ (*House Judiciary Committee Republicans*, 22 Nisan 2015) <<http://judiciary.house.gov/usa-freedom-act>> Erişim Tarihi: 05.02.2025.

Mahkemesi'nin konu hakkındaki beyanının kamuya açılmasıyla ortaya çıkmıştır.⁴⁷ Bu gelişme, ABD merkezli teknoloji şirketlerindeki kullanıcı verilerine erişmek için NSA nezdinde bir arka kapı (*backdoor*) olarak *PRISM* kod adlı programın kullanıldığı iddiasıyla başlayan sürecin baş aktörü olan *Edward Snowden* tarafından ileri sürülen iddialarla da paralellik içermektedir.⁴⁸

Rusya'da 2009 yılında yürürlüğe giren ve devamındaki değişikliklerle şekillenen Bilgi, Bilgi Teknolojileri ve Bilginin Korunması Hakkında Federal Yasa (*Federal Law On Information, Information Technologies and Protection of Information*), Rusya'nın internet üzerindeki denetim ve gözetim faaliyetlerinin genel hukuki dayanağıdır.⁴⁹ Rusya Federal Bilgi Teknolojileri ve Kitle İletişim Denetleme Kurumu (*Roskomnadzor*), ilgili süreçleri yürüten devlet organıdır.⁵⁰ *SORM* kısaltmasıyla bilinen "Operasyonel Soruşturma Faaliyetleri Sistemi" de başta Federal Güvenlik Sevisi (*FSB*) olmak üzere ilgili devlet kurumlarınca ağ gözetiminin etkili bir enstrümanı olarak kullanılmaktadır.⁵¹ *SORM*, 1995 tarihli Operasyonel Arama Faaliyetleri Federal Yasası'na⁵² dayanmaktadır. Yasanın kapsamı yıllar içinde genişletilmiştir. Diğer taraftan 2016'da kabul edilen ve Yarovaya Yasaları adıyla bilinen düzenlemelerle hizmet sağlayıcıların veri ve metaveri saklama yükümlülüklerinde süre uzatımına gidilmiş, mesajlaşma uygulamalarında şifreli arka kapılar bulundurulması zorunlu tutulmuştur.⁵³

Türkiye'de genel internet denetimi Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yürütülmektedir.⁵⁴ Ayrıca Milli İstihbarat Teşkilatı'na (MİT), 2014'te kabul edilen değişiklikle "dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini

⁴⁷ Greg Nojeim, 'FISA Court Opinion Outlines FBI Abuse of Key Intelligence Surveillance Authority' (*Center for Democracy and Technology*, 4 Eylül 2020) <<https://cdt.org/insights/fisa-court-opinion-outlines-fbi-abuse-of-key-intelligence-surveillance-authority/>> Erişim Tarihi: 05.02.2025. ABD Ulusal İstihbarat Direktörlüğü Ofisi'nin (*Office of the Director of National Intelligence-ODNI*) verdiği yetkiyle kamuya açılan FISA Mahkemesi beyanı ve emir için bkz Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, (6 Aralık 2019) <https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf> Erişim Tarihi: 05.02.2025.

⁴⁸ Katie Sanders, 'Fact-Checking John Oliver's Interview with Edward Snowden about NSA Surveillance' (*PolitiFact*) <<https://www.politifact.com/factchecks/2015/apr/09/edward-snowden/fact-checking-john-olivers-interview-edward-snowde/>> Erişim Tarihi: 05.02.2025.

⁴⁹ Bilgi Yasası adıyla da anılan yasanın İngilizce çevirisi için bkz 'Federal Law No. 149-FZ of July 27, 2006, on Information, Information Technologies and Protection of Information (as Amended up to Federal Law No. 222-FZ of July 21, 2014)' (*WIPO Lex*) <<https://www.wipo.int/wipolex/en/text/371388>> Erişim Tarihi: 05.02.2025.

⁵⁰ Andrei Richter, 'Regulation of Social Media in Russia' (European Audiovisual Observatory 2021) 9.

⁵¹ Andrei Soldatov and Irina Borogan, 'Russia's Surveillance State' (2013) 30 *World Policy Journal* 23, 25; Nathalie Maréchal, 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy' (2017) 5 *Media and Communication* 29, 33.

⁵² Federal law No. 144-FZ of 12 August 1995, m 8; Kanun metninin İngilizce çevirisi için bkz 'Federal Law No. 144-FZ Of August 12, 1995 On Operational-Search Activities (with the Amendments and Additions of July 18, 1997, July 21, 1998, January 5, December 30, 1999, March 20, 2001, January 10, June 30, 2003, June 29, August 22, 2004, December 2, 2005, July 24, 2007)' (*World Trade Organization*) <https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_373.pdf> Erişim Tarihi: 05.02.2025.

⁵³ Maréchal (n 51) 34.

⁵⁴ 'Denetleme' (BTK) <<https://www.btk.gov.tr/denetleme>> Erişim Tarihi: 05.02.2025.

kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak” yetkisi verilmiştir.⁵⁵ Diğer yandan hemen her ülkede benzerleri olduğu üzere BTK ve Ulusal Siber Olaylara Müdahale Merkezi (USOM), internet ortamında karşılaşılan hukuka aykırılıklara yönelik çevrimiçi ihbar hizmeti sunmaktadır.⁵⁶

İnternetin devletlerin gözetiminde olması, günümüzde bir sır olarak görülmemektedir. Devletler, hukuk düzenlemeleri ve teknik kapasiteleri ölçüsünde veri toplama ve değerlendirme süreçlerini yürütmektedir. Çoğu durumda ise bunun için hizmet sağlayıcılardan bilgi talep edilmektedir. Çocuk istismarı ve uyuşturucu ticareti gibi vakalarda hizmet sağlayıcılar ilgili devlet makamlarına kendiliğinden bilgi verebilirken, bilhassa ölüm veya ciddi yaralamaya ilişkin tehlike durumlarında acil bilgi taleplerine de karşılık verilebilmektedir.⁵⁷ Şifreli iletişim ise gözetim meselesinin çekirdeğini oluşturan hususlardandır. Özel hayatın ve iletişimin mahremiyeti gereği şifreli iletişim kural olarak serbest olsa dahi içeriğine asla erişilemeyecek şekilde şifrelenmiş iletişim araçlarına karşı devletlerin -en azından- mesafeli olması doğaldır. Hizmet sağlayıcılara en sık talep ileten devletlerden biri olan Hindistan örneğinde, 2000 tarihli Bilgi Teknolojisi Yasası (*The Information Technology Act*)⁵⁸ ile devletin güvenliği, kamu düzeni, yabancı devletlerle dostane ilişkilerin sürmesi ve suçun önlenmesi gibi gerekçelere dayalı talep durumunda şifreli iletişim içeriğinin devlete bildirilmesi zorunlu kılınmıştır. Bu durumlarda şifre çözümünden imtina edilmesi ise hapis cezasına tabi tutulmuştur.⁵⁹ ABD’de Kolluk Kuvvetleri için İletişim Yardımı Yasası (*Communications Assistance for Law Enforcement Act-CALEA*)⁶⁰ ve Rusya’da Yarovaya Yasaları benzer yetkiler öngörmektedir. Çin’e gelindiğinde Siber Güvenlik Yasası, Kriptografi Yasası⁶¹ ve Kamu Güvenlik Kurumları Tarafından İnternet Güvenliği Gözetim ve Denetimine İlişkin Yönetmelik⁶² gibi düzenlemelerle dijital ve şifreli iletişimin sıkı gözetim altına alındığı görülmektedir. Uçtan uca şifreleme hizmeti sunan mesajlaşma uygulamalarında ise ne hizmet sağlayıcının ne devletin

⁵⁵ 1.11.1983 tarih ve 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanununda Değişiklik Yapılmasına Dair Kanun (RG 26.4.2014/28983), m 1.

⁵⁶ Hizmetlere erişim için sırasıyla bkz ‘İnternet İhbar Başvurusu’ (*BTK*) <<https://www.turkiye.gov.tr/btk-internet-ihbar-basvurusu>> Erişim Tarihi: 05.02.2025; ‘İhbar’ (*USOM*) <<https://www.usom.gov.tr/ihbar>> Erişim Tarihi: 05.02.2025.

⁵⁷ En yaygın kullanılan sosyal medya platformlarından X ve Instagram örneklerinde, işletmecilerin devletlerle bilgi paylaşımına dair belirledikleri esaslar için sırasıyla bkz Erişim Tarihi: 05.02.2025; ‘Kolluk Kuvvetlerine Yönelik Bilgiler’ (*Instagram*) <<https://help.instagram.com/494561080557017>> Erişim Tarihi: 05.02.2025.

⁵⁸ Yasa metnine ve 2008 tarihli değişikliklere erişim için bkz ‘Rules and Procedures-Central’ (*GeM-CPPP*) <<https://eprocure.gov.in/cppp/rulesandprocs>> Erişim Tarihi: 05.02.2025.

⁵⁹ Hindistan Bilgi Teknolojisi Yasası, m 69.

⁶⁰ Communications Assistance for Law Enforcement Act, 47 U.S. Code §§ 1001–1010 (1994).

⁶¹ Yasanın İngilizce çevirisi için bkz Todd Kuhns, ‘Cryptography Law of the People’s Republic of China’ (*AppInChina*, 1 Ocak 2020) <<https://appinchina.co/government-documents/cryptography-law-of-the-peoples-republic-of-china/>> Erişim Tarihi: 05.02.2025.

⁶² Yönetmeliğin İngilizce çevirisi için bkz Rogier Creemers, ‘Regulations on Internet Security Supervision and Inspection by Public Security Bodies’ (*DigiChina*, 15 Eylül 2018) <<https://digichina.stanford.edu/work/regulations-on-internet-security-supervision-and-inspection-by-public-security-bodies/>> Erişim Tarihi: 05.02.2025.

mesaj içeriklerine erişim imkânı bulunmaktadır.⁶³ Devletlerin bilgi paylaşımına dair zorlayıcı hükümlerini bu alana genişletmeleri ve caydırıcı yaptırımlar öngörmeleri halinde, söz konusu hizmet sağlayıcılar ya şifreleme prosedürlerini esneterek veri çıkışı için kapı açmak ya da ilgili devletin ülkesindeki faaliyetlerine son vermek durumunda kalacaktır.⁶⁴

B. İçerik Kaldırma

İnternet üzerinde husule gelen hukuka aykırılıkların türüne göre fail, fiil ve durum hakkındaki önlemler değişkenlik gösterir. Devlet, kişiler üzerindeki yetkisini kullanmak suretiyle suç veya haksız fiil failine ulusal hukukunu uygulayabilmektedir. Benzer durum, eşya üzerindeki ülkesel yetki kullanımında da geçerlidir. İnternetteki mantıksal unsurlar söz konusu olduğunda ise ulusal hukukun icrasını “doğrudan” gerçekleştirmek çoğu devlet için mümkün değildir.

Bir içeriğin internet aracılığıyla erişilebilir olmasının hukuka aykırılığı durumunda, bir taraftan hukuka aykırılığa sebep olan fail hakkında yetki tespit ve icrası gündeme gelirken diğer taraftan hukuka aykırı durumun sona erdirilmesi için ilgili içeriğin “erişilemez” hale getirilmesi gerekmektedir. İnternetin yapısı itibarıyla bir içeriğin erişilemez hale gelmesinin birincil yolu, bulunduğu sunucudan “kaldırılmasıdır”. Bu sonucun sağlanması ise öncelikle fiili imkanlara bağlıdır. Kaldırma eylemini gerçekleştirebilecek süjeler, kullanılan platforma göre değişebilir. Web için konuşulduğunda, bazı sitelerinin mimarisinin içerik sağlayan kişiye sonradan içeriği kaldırma imkânı tanıması mümkündür. Diğer yandan, kişilerin kendi cihazlarını sunucu olarak kullandığı adem-i merkezîyetçi dosya paylaşım platformlarında içerik ancak bu kişiler tarafından kaldırılabilir. İçerik kaldırmanın uygulamada en sık gerçekleştiği alanlar olan sosyal medya platformları ve depolama hizmetlerinde ise hem hizmet hem içerik sağlayıcılar, içeriği kaldırma imkânına sahiptir. Her durumda, devletler, ülkelerindeki sunuculara fiziksel olarak ve ülke dışındaki sunuculara bilgi ve iletişim teknolojilerinin kullanımı yoluyla cebren erişerek müdahale etme fiili imkânına sahiptir. Fakat devletin, ülkesi dışındaki sunucuya cebren yetkisiz erişimi, müdahale yasağına aykırılık teşkil etmesi bakımından, -sunucu, devlet dışı aktöre ait olsa dahi- sunucuyu ülkesinde bulunduran devletin egemenliğini ihlal edecek nitelikte bir siber faaliyet olarak görülebilir. Zira kolluk, ülkelerinde gerçekleştirilmesinde devletlerin münhasıran yetkili oldukları bir faaliyet tipidir.⁶⁵ Sunucunun uzayda yahut açık denizdeki bir platformda olması gibi durumlarda dahi yer sağlayıcının uyrukluk ile bağlı olduğu devlet,

⁶³ Söz konusu durum, hizmet sağlayıcıların sistemlerini vaat ettikleri şekilde işlettikleri ve gizli bir arka kapı kullanmadıkları varsayımında geçerlidir.

⁶⁴ Böyle bir gelişmenin Türkiye’de gerçekleşmesinin önüne geçilmesi yönünde sivil toplum kuruluşları ve şirketlerden oluşan bir grup tarafından bir çağrı metni yayınlanmıştır; ‘Türkiye: Uçtan Uca Şifreleme Korunmalı’ (ARTICLE 19, 20 Nisan 2023) <<https://www.article19.org/tr/resources/turkey-protect-end-to-end-encrypted-services/>> Erişim Tarihi: 05.02.2025. Şifreli iletişim süreçlerinde arka kapıya teknik olarak sağlanması, tabii ki uygulamada çeşitli süjelerce ve farklı yollarla istismar edileceğine yönelik kaygıları beraberinde getirecektir. Ancak milli güvenliğe, kamu düzenine ve insan haklarına ilişkin birçok yüksek menfaatin, söz konusu hususta hukuka dayalı olarak birtakım esnemeleri zamanla zaruri kılacağını öngörmek mümkündür.

⁶⁵ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 22.

diplomatik koruma müessesesine dayanarak fail devletin uluslararası sorumluluğunu ileri sürebilecektir.⁶⁶

Uygulamada devletler genellikle içeriğin kaldırılması için hizmet sağlayıcılara başvurma yolunu izlemektedir. Belli başlı sorunların da doğrudan devlet müdahalesine gerek olmadan öncelikle internet sükjeleri arasında çözümlüne imkân tanınmıştır. Bilhassa fikri mülkiyet gibi hak ihlallerinin yargıya aksetmeden sona erdirilmesi adına ABD’de Dijital Binyıl Telif Hakkı Yasası (*Digital Millennium Copyright Act-DMCA*) ile hukuk alanına giren “uyar ve kaldır (*notice and takedown*)” prosedürü, hukuka aykırı içerik karşısında aracı hizmet sağlayıcıların sorumluluklarını sınırlamakla birlikte içeriğin kaldırılması için kullanıcı, devlet ve hizmet sağlayıcı arasında bir iş birliği zemini kurmuştur.⁶⁷ Bu sayede aracı hizmet sağlayıcı, platformundaki tüm içerikleri anbean izleme ve olası hukuka aykırılıkta doğrudan sorumlu tutulma gibi ağır külfetlerden kurtulmuştur. Uyar ve kaldır prosedüründe, bir içerik nedeniyle haklarının ihlal edildiğini düşünen kişi, aracı hizmet sağlayıcıya bildirimde bulunur. Böylece hem aracı hizmet sağlayıcı hukuka aykırılıktan haberdar edilmiş olur hem içeriğin kaldırılması pratik, hızlı ve verimli bir süreç sonucunda sağlanır. Aracı hizmet sağlayıcılar, içeriğin hukuka veya kendi politikalarına aykırı olduğuna kanaat getirirse, içerik sağlayıcıyı bilgilendirip içeriği kaldırmasını isteyebilir, konu hakkındaki savunmasını talep edebilir yahut içeriği doğrudan kaldırabilir. Bildirime rağmen içerik kaldırılmazsa bu kez başta yargı olmak üzere devlet organlarına başvurulur. Gelgelelim bu mekanizma zaman zaman, teoride umulduğu gibi sağlıklı işlememektedir. Bildirim sonucunda hizmet sağlayıcılar, yasadışı içeriği meşru bularak platformlarında tutmaya devam edebilmekte yahut aslında hukuka uygun olan bir içeriği meşru bulmayarak kaldırabilmektedir. Dolayısıyla literatürde uyar ve kaldır prosedürü, aracı hizmet sağlayıcılar bakımından keyfilik zeminine oturması nedeniyle eleştirilmiştir.⁶⁸

İçerik kaldırılması sürecine devletlerin dahli, ilgili kurumlarının internet sükjelerine talimatta bulunması ya da bir mahkeme kararının icrası yoluyla gerçekleşebilir. Türkiye örneğinde, söz konusu işlem için 5651 Sayılı Kanun metninde “içeriğin yayından çıkarılması” tabiri ve “içerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılması” tanımı tercih edilmiştir.⁶⁹ Kanunda birtakım suçlar belirlenmiş ve bu

⁶⁶ UAD, Barcelona Traction Davası’nda şirketlerin uyrukluğunda olduğu devletin diplomatik koruma hakkının mevcudiyetini kabul etmiştir; Sümeyra Sena Kurt, ‘Uluslararası Hukukta Diplomatik Koruma’ (2020) 6 Anadolu Üniversitesi Hukuk Fakültesi Dergisi 467, 488.

⁶⁷ Domingos Soares Farinho and Ricardo Resende Campos, ‘Models of Legal Liability for Social Networks: Between Germany and Portugal’ in Carlos Blanco de Moraes, Gilmar Ferreira Mendes and Thomas Vesting (eds), *The Rule of Law in Cyberspace* (Springer 2022) 334.

⁶⁸ Jennifer Urban and Laura Quilter, ‘Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act’ (2006) 22 Santa Clara High Technology Law Journal 621, 623; Aleksandra Kuczerawy, ‘From “Notice and Takedown” to “Notice and Stay Down”: Risks and Safeguards for Freedom of Expression’ in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 532; Päivi Korpisaari, ‘From Delfi to Sanchez – When Can an Online Communication Platform Be Responsible for Third-Party Comments? An Analysis of the Practice of the ECtHR and Some Reflections on the Digital Services Act’ (2022) 14 Journal of Media Law 352, 373–374.

⁶⁹ 5651 sayılı Kanun, m 2/1-ö.

suçların oluştuğuna dair yeterli şüphe sebebi bulunan içeriğin kaldırılabilceği öngörülmüştür.⁷⁰ İçeriğin çıkarılması kararı, soruşturma aşamasında hâkim ve kovuşturma aşamasında mahkeme tarafından verilebilmektedir.⁷¹ Ayrıca başta belli suç tipleri için BTK Başkanı'na re'sen içeriğin çıkarılması kararı verme yetkisi tanınmış olsa da bu yetki, suç tespitine bağlı bir nihai tedbirin yargı kararı olmaksızın uygulanmasının masumiyet karinesine aykırı düştüğünden bahisle Anayasa Mahkemesi'nce (AYM) iptal edilmiştir.⁷² Mevcut durumda BTK Başkanı, gecikmesinde sakınca bulunan hallerde istisnai şekilde içeriğin çıkarılması kararı verebiliyor olsa da bu kararların yine hakim onayına sunulması gerekmektedir.⁷³ Yine aynı hallerde Cumhurbaşkanlığı veya ilgili bakanlıkların talebiyle de BTK Başkanı söz konusu yöntemi uygulayabilmektedir.⁷⁴

Çin'de Siber Güvenlik Yasası hükümleri, yetkili kurumların hukuka aykırı içeriğin iletiminin durdurulmasını, silinmesini ve ilgili kayıtların saklanması hizmet sağlayıcılardan talep edebileceğini;⁷⁵ hizmet sağlayıcıların kendi tespit ettikleri hukuka aykırı içerik veya yetkili kurumların hukuka aykırı içeriğe ilişkin talepleri hakkında gerekli önlemleri almadıkları takdirde para cezası, işletmenin durdurulması ve ruhsat iptali gibi yaptırımlara maruz kalacaklarını düzenlemektedir.⁷⁶ Uygulamada Çin Siber Uzay İdaresi'nin, hizmet sağlayıcılara karşı önceleri genellikle kınama ve ifşa etme gibi yöntemlere başvurduğu fakat 2020 yılının sonlarından itibaren yaptırımların sıklaştığı ve ağırlaştığı aktarılmıştır.⁷⁷

Rusya'da içerik kaldırmaya dair esaslar, "Bilgi Yasası" adıyla bilinen "Bilgi, Bilgi Teknolojileri ve Bilginin Korunması Hakkında Federal Yasa"⁷⁸ hükümlerince düzenlenmiştir. Bilgi Yasası'nda, mahkeme kararıyla "Rusya Federasyonu'nda yayılması yasak bilgi" olarak kabul edilenlerin yanı sıra çocukların korunması ile narkotik maddelerin, intiharın ve yasadışı

⁷⁰ 5651 sayılı Kanun, m 8/1.

⁷¹ 5651 sayılı Kanun, m 8/2.

⁷² AYM, E 2020/76, K 2023/172, T 11/10/2023, § 86.

⁷³ 5651 sayılı Kanun, m 8/2; "(1) Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Cumhurbaşkanlığı veya milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Başkan tarafından internet ortamında yer alan yayınlı ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir. Karar, Başkan tarafından derhâl erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilir. İçerik çıkartılması ve/veya erişimin engellenmesi kararının gereği, derhâl ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir. (2) Cumhurbaşkanlığı veya ilgili Bakanlıkların talebi üzerine Başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, Başkan tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi hâlde, karar kendiliğinden kalkar."

⁷⁴ 5651 sayılı Kanun, m 8/A; "(1) ...Cumhurbaşkanlığı veya milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Başkan tarafından internet ortamında yer alan yayınlı ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir..."

⁷⁵ Çin Siber Güvenlik Yasası, m 50.

⁷⁶ Çin Siber Güvenlik Yasası, m 68-69.

⁷⁷ Huyue Zhang (n 40) 145–149.

⁷⁸ The Russian Federation Federal law No. 149-FZ of 14 July 2006. <https://eais.rkn.gov.ru/docs.eng/149.pdf> (31.12.2024).

kumarın önüne geçilmesini amaçlayan hükümlere aykırılığı tespit edilen içerikleri barındıran siteler için Roskomnadzor nezdinde bir sicil oluşturulması;⁷⁹ bu sicile eklenen sitelerin işletmecilerine yer sağlayıcılar tarafından 24 saat içinde bildirimde bulunulması,⁸⁰ site işletmecilerinin de bildirimi aldıktan sonraki 24 saat içinde içeriği kaldırması yükümlülüğü getirilmiştir.⁸¹ Site işletmecisinin bildirimde uymaması halinde ise yer sağlayıcının yine 24 saat içinde siteye erişimi kısıtlama yükümlülüğü doğacaktır.⁸² Şayet yer sağlayıcı da yükümlülüğünü yerine getirmezse bu husus sicile işlenecek ve İSS'ler 24 saat içinde siteye erişimi engelleyecektir.⁸³ Site işletmecilerinin söz konusu sicile kayıt kararı alınmasından itibaren üç ay içinde yetkili mahkemeye itiraz hakları bulunmaktadır.⁸⁴ Sicil uygulamasının yanı sıra fikri mülkiyet ihlallerinde kesinleşmiş mahkeme kararına istinaden hak sahiplerince;⁸⁵ kamu düzeni ve milli güvenliğin korunmasına ilişkin durumlarda bütün ilgililerce Roskomnadzor'a yapılacak başvuru ile içerik kaldırma prosedürü başlatılabilmektedir.⁸⁶

Devletler, içerik kaldırma yetkilerini hangi organlarıyla icra edeceklerini, yukarıdaki örneklerde de görüldüğü üzere ulusal hukuklarında belirlerler. Akdedilecek bir uluslararası antlaşma ile uygulamada yeknesaklık sağlanabilecek olsa da devletlerin internetin işleyişine ilişkin yaklaşım farklılıkları hasebiyle böyle bir antlaşmanın henüz uzak bir ideal olduğu söylenebilir. Genel uygulama, içerik kaldırma karar ve talimatlarının, içerik ve yer sağlayıcılara bildirilmesi ve gereğinin yerine getirilmesinin beklenmesi yönündedir. Hatta Çin örneğinde hizmet sağlayıcıların hukuka aykırı içeriği proaktif olarak tespit etmesi, raporlaması ve kaldırması beklenmektedir.⁸⁷ Pratik güçlük ise ülke dışından hizmet veren yer ve hizmet sağlayıcılar ile yabancı içerik sağlayıcıların söz konusu kararları yerine getirmemeleri durumunda yaşanmaktadır. Devletler bu gibi durumlarda aşamalı olarak para cezası, erişim engeli, lisans iptali gibi yollara başvurabilmektedir. Son noktada fiilen en uygulanabilir yöntem İSS'ler aracılığıyla erişimin engellenmesi olsa dahi erişim engelinin de etkisi sınırlı kalmaktadır. Sonuçta teknik imkanlara ve ihdas edilen kurumlara rağmen içeriğe müdahale hususunda devlet kabiliyetlerinde büyük bir sıçrama yaşandığını söylemek güçtür. Esas işleyiş hâlen, içerik kaldırılmasının doğrudan içeriğe yönelik cebren devlet müdahalesiyle sağlanmasındansa muhataplara yönelik yaptırımlar ya da yaptırım tehditleriyle sağlanması yönündedir.

⁷⁹ Rusya Bilgi Yasası, m 15.1.

⁸⁰ Rusya Bilgi Yasası, m 15.1/7.

⁸¹ Rusya Bilgi Yasası, m 15.1/8.

⁸² Rusya Bilgi Yasası, m 15.1/8.

⁸³ Rusya Bilgi Yasası, m 15.1/10.

⁸⁴ Rusya Bilgi Yasası, m 15.1/6.

⁸⁵ Rusya Bilgi Yasası, m 15.2.

⁸⁶ Rusya Bilgi Yasası, m 15.3.

⁸⁷ Çin Halk Cumhuriyeti, Çevrimiçi Bilgi İçeriği Ekosisteminin Yönetişimine İlişkin Hükümler (Çin Siber Uzay İdaresi, 5 Numaralı Emir) m 36 vd; Hükümlerin İngilizce çevirisi için bkz Joan Barata and Bolin Zhang, 'Provisions on the Governance of the Online Information Content Ecosystem' (WILMAP) <<https://wilmap.stanford.edu/entries/provisions-governance-online-information-content-ecosystem>> Erişim Tarihi: 05.02.2025.

C. Filtreleme ve Erişim Engeli

Hukuka aykırılık durumlarında sunuculara ve süjelere müdahale imkânı bulamayan devletler için en pratik çözüm, halihazırda egemenlikleri altında bulunan kurumsal İSS’ler marifetiyle ilgili içerikleri filtrelemek yahut içeriklere erişimi engellemektir. Söz konusu önlem, içeriğin bulunduğu sunucu ile kullanıcı arasındaki bağın kesilmesini ifade etmektedir. 5651 sayılı Kanun’da da erişimin engellenmesinin, “*Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesi*” anlamına geldiği belirtilmiştir.⁸⁸ Kanun böylece erişim engeli türlerini de açık uçlu olarak saymış bulunmaktadır. Filtreleme ise belli türlerdeki içeriklerin belli kullanıcı gruplarına ulaşmasının engellenmesidir. Kullanıcılar, istenmeyen içeriklere maruz kalmamak için kendi iradeleriyle filtreleme programları kullanabilirken, devletler de içerik bazlı erişim engelinin diğer bir ifade şekli olarak filtreleme önlemine başvurabilmektedir.

Gözetim, denetim, filtreleme ve erişim engeli kombinasyonunun dünyadaki en meşhur sistematik uygulaması, Çin’de işleyen ve literatürde Çin Seddi’ne ithafen “Çin Güvenlik Seddi (*The Great Firewall of China*)” adıyla anılan sistemdir. Sistem, internet trafiğini ve paketlerin içeriğini inceleyebilmekte, yasak olan içeriğe erişimi bu yolla engellemektedir. Çin’deki uygulamaların zamanın gereğine göre sıkılaşılabildiği, sanal özel ağ (*virtual private network-VPN*) hizmetlerine ve hatta gizlice VPN hizmeti veren Web sitelerine dahi erişimin engellenebildiği, gerek görüldüğünde kullanıcının maksadının anlaşılması adına ifadesinin alınabildiği aktarılmıştır.⁸⁹

Rusya’da hukuka aykırı içeriğe erişimin engellenmesi, yukarıda içeriğin kaldırılması hususunda aktarılan işeyiş ile paralel biçimde yürütülmektedir. Belli içerik türleri hakkında mahkeme kararı ya da savcılık emri olmaksızın Roskomnadzor’a tanınan kaldırma yetkisi, erişim engeli için de geçerlidir. Rus internet altyapısında belli noktalarda bulunan ve Moskova’daki komuta merkezince kontrol edilen “kırmızı kutu” donanımları, ülkenin herhangi bir bölgesindeki internet trafiğinin yavaşlatılmasında, erişim engeline ve bilgi akışının yeniden yönlendirilmesinde kullanılmaktadır.⁹⁰

Türkiye’de erişimin engellenmesi kararı, içeriğin çıkarılması kararıyla beraber anılarak düzenlenmiştir. İçeriğin çıkarılmasına dair yukarıda değinilen AYM kararı, BTK Başkanı’nın erişim engelleme yetkisine karşı bir tasarrufta bulunmamıştır. Erişim engelinin, engellenen hizmetin türüne göre kalıcı veya belirli süreli olarak getirilmesi mümkündür.⁹¹ Erişim engelinin dolaylı bir uygulaması olarak internet trafiği bant genişliğinin daraltılmasına da 5809 sayılı Elektronik Haberleşme Kanunu hükmüne⁹² dayanarak başvurulabilmektedir. Ayrıca güncel

⁸⁸ 5651 Sayılı Kanun, m 2/1-o.

⁸⁹ James Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (2nd edn, Zed 2021) 28.

⁹⁰ Richter (n 50) 7.

⁹¹ 5651 sayılı Kanun, m 8/2.

⁹² 5809 sayılı Kanun, m 60/10; “*Anayasanın 22’nci maddesinde sayılan sebeplerden biri veya birkaçına bağlı*

örneklerden olan Instagram Web sitesine erişim engeli kararında olduğu gibi, ilgili internet süjesinin ulusal hukuka uygun davranacağını taahhüt etmesi sonucunda engel kaldırılabilir. ⁹³ 2024 Ekim ayında Brezilya'nın, X Web sitesine getirdiği erişim engelini altı hafta sonra kaldırması da benzer bir başka süreç örneğidir. ⁹⁴

ABD'de erişim engeli uygulaması farklı yasalara dayanılarak yargı kararıyla icra edilmektedir. *DMCA*, Çocukların İnternette Korunması Yasası (*Children's Internet Protection Act-CIPA*), ⁹⁵ Devletlerin ve Mağdurların Çevrimiçi Seks Ticaretiyle Mücadele Etmesine İzin Yasası (*Allow States and Victims to Fight Online Sex Trafficking Act*) ve Seks Tacirlerine Müsaadeyi Durdurma Yasası (*Stop Enabling Sex Traffickers Act*) (*FOSTA-SESTA*) ⁹⁶ gibi düzenlemeler, içeriğin türüne göre önlemler öngörür. Nisan 2024'te ABD Temsilciler Meclisi'nden geçen, Amerikalıları Yabancı Hasım Kontrolündeki Uygulamalardan Koruma Yasası (*Protecting Americans from Foreign Adversary Controlled Applications Act-PAFACA*) ⁹⁷ ise ABD Başkanı yahut ilgili birimler tarafından “yabancı hasım kontrolünde”

olarak, gecikmesinde sakınca bulunan hâllerde Cumhurbaşkanlığı, alınması gereken tedbirleri belirler ve uygulanmak üzere Kuruma bildirir. Kurum Başkanı, Cumhurbaşkanlığının gerekli gördüğü tedbirlere ilişkin kararını...”. Söz konusu uygulamaya yine 5809 sayılı Kanun'da şebekeler üstü hizmet sağlayıcılar için öngörülmüş bir yaptırım olarak değinilmiş olsa da erişim engelini ikame edici bir önlem olarak bant daraltma yöntemi doğrudan zikredilmemiştir. Ayrıca erişim engeli tanımına dair yukarıda aktarılan 5651 sayılı Kanun hükmündeki “ve benzeri yöntemler” ibresinin, bu uygulamaya dayanak teşkil edip edemeyeceği teknik olarak tartışmaya açık görünmektedir.

⁹³ ‘Instagram’a Uygulanan Erişim Engeli Kaldırıldı’ (*Anadolu Ajansı*, 11 Ağustos 2024) <<https://www.aa.com.tr/tr/info/infografik/40694>> Erişim Tarihi: 05.02.2025. Her ne kadar erişim engeli kararının gerekçesi olarak söz konusu Web sitesi işletmecisinin hukuka aykırı içeriklerin kaldırılması konusunda gerekli önlemleri almaktan kaçınmakta ısrar etmesi gösterilse de hukuka uygun içeriklerin Web sitesi işletmecisi tarafından kurum politikası gerekçesiyle kaldırılması ve bu suretle özel sansür uygulanması da tetikleyici faktör olmuştur; Serhat Tutak, ‘Bakan Uraloğlu, Instagram’a Getirilen Erişim Engeline İlişkin Son Durumu Değerlendirdi’ (*Anadolu Ajansı*, 6 Ağustos 2024) <<https://www.aa.com.tr/tr/bilim-teknoloji/bakan-uraloglu-instagram-a-getirilen-erisim-engeline-iliskin-son-durumu-degerlendirdi/3296674>> Erişim Tarihi: 05.02.2025.

⁹⁴ ‘Elon Musk’s X to Be Reinstated in Brazil after Complying with Court’ (*Euronews*, 9 Ekim 2024) <<https://www.euronews.com/next/2024/10/09/elon-musks-x-to-be-reinstated-in-brazil-after-complying-with-court>> Erişim Tarihi: 05.02.2025. Vakanın dikkat çekici bir yönü de Brezilya’da aktif olarak erişim sağlayıcılık hizmeti veren Starlink’in bağlı olduğu SpaceX şirketinin, söz konusu karara uyarak “X” Web sitesine erişimi engellemesidir. SpaceX ve X şirketleri ayrı tüzel kişilikler olsa da günümüzün önde gelen teknolojik iktidar sahiplerinden Elon Musk’ın yönetimi altındadırlar. SpaceX, sahip olduğu teknik avantajlara rağmen Brezilya makamlarının kararını uygulamış, sunduğu hizmetin meşruiyetini muhafaza yoluna gitmiştir. Yaşanan bu gelişmeler, internet süjelerinin, ellerindeki fiili imkanlardan bağımsız olarak ilgili devletlerin otoritelerine uymak suretiyle meşru zeminde kalmaktaki menfaatlerinin, hukukun tatbik edilebilirliğindeki kritik önemine işaret etmektedir; Muhammed Enes Çallı, ‘Starlink to Comply with Court Orders to Block X in Brazil’ (*Anadolu Ajansı*, 4 Eylül 2024) <<https://www.aa.com.tr/en/world/starlink-to-comply-with-court-orders-to-block-x-in-brazil/3320971>> Erişim Tarihi: 05.02.2025.

⁹⁵ Yasa hakkında resmi bilgilendirme için bkz ‘Children’s Internet Protection Act (CIPA) | Federal Communications Commission’ (*Federal Communications Commission*, 5 Temmuz 2024) <<https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>> Erişim Tarihi: 05.02.2025.

⁹⁶ Stop Enabling Sex Traffickers Act, Public Law No 115-164, 132 Stat 1253 (11 Nisan 2018).

⁹⁷ Yasa teklifine ve yasama sürecine dair bilgi için bkz ‘H.R.7521 - 118th Congress (2023-2024): Protecting Americans from Foreign Adversary Controlled Applications Act’ (*Congress*, 14 Mart 2024) <<https://www.congress.gov/bill/118th-congress/house-bill/7521>> Erişim Tarihi: 05.02.2025.

olduğu tespit edilen uygulamaların (yazılım, Web sitesi, mobil uygulamalar vs.) kullanımının belli süre içinde yasaklanmasını düzenlemektedir. Halihazırda yabancı hasım kapsamına giren devletler Kuzey Kore, Çin, Rusya ve İran'dır.⁹⁸ Bilhassa Çin menşeli TikTok uygulamasına karşı gündeme gelen yasa, içeriğin türüne değil kaynağına ve hatta bizzat yer sağlayıcısının kimliğine göre engelleme öngörmesi bakımından sıra dışı niteliktedir. Yasanın yürürlüğe girmesi halinde, kastedilen türdeki uygulama sahiplerinin uygulamalarını satmak ve ABD'de hizmet sunamamak arasında bir seçime zorlanacağı belirtilmiştir.⁹⁹

İnternet içeriğinin tamamen özgür ve devlet denetiminden azade olması artık mümkün ve makul görünmemektedir. Hatta İSS'ler dahi kara liste gibi uygulamalarla devlet ile kullanıcı arasındaki noktada kendiliğinden denetim ve engelleme faaliyeti gerçekleştirebilmektedir.¹⁰⁰ İçeriğe devlet müdahalesinin sınırları da hemen her ülke için özellikle insan hakları bağlamında yoğun tartışmaların konusudur. Uygulamadaki zorluklar ise sorunun bir diğer cephesidir. Kaldırılan içerik neredeyse anında tekrar internette erişilebilir hale gelmekte, erişim engelleri ise gerek kullanıcılar gerek engele maruz kalmış Web sitesi işletmecileri veya yer sağlayıcılar tarafından başvuru yöntemlerle aşılabilmektedir. VPN veya vekil (*proxy*) sunucular, kullanıcıların en yaygın tercih ettiği araçlardır. Diğer taraftan bir alan adı engellendiğinde hemen benzer yenisini hizmete sunmak ve bu döngüyü sürekli hale getirmek (Türkiye'de bilhassa popülerlik kazanmış korsan yayın, yasadışı bahis ve kumar gibi içerikleri sunan Web sitelerinde de yaygın şekilde görüldüğü üzere) de hizmet sağlayıcıların en sık tercih ettiği yollardandır. Sözgelimi xyz.abc alan adlı Web sitesine erişim engellendiğinde, aynı site içeriği sırasıyla xyz1.abc, xyz2.abc gibi sonu gelmeyen alan adı kombinasyonları ile tekrar hizmete sunulmaktadır. Devletler adına ortaya çıkan durum, *Post*'un çekiçle köstebek vurma oyunu benzetmesini haklı çıkarır niteliktedir.¹⁰¹

⁹⁸ 10 U.S. Code § 4872(d)(2).

⁹⁹ Sapna Maheshwari, David McCabe and Annie Karni, 'House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App' *The New York Times* (13 Mart 2024) <<https://www.nytimes.com/2024/03/13/technology/tiktok-ban-house-vote.html>> Erişim Tarihi: 05.02.2025.

¹⁰⁰ Mevcut fikri mülkiyet rejimlerine karşı politik hareketin merkezi olarak görülen The Pirate Bay topluluğu (bkz Jessica Lucia Beyer, *Expect Us: Online Communities and Political Mobilization* (Oxford University Press 2014) 65.) tarafından kurulan <<https://thepiratebay.org>> alan adlı Web sitesi (P2P dosya paylaşım protokollerinden Torrent'in dünyadaki en popüler izleyicilerindendir, *tracker* bu hususta Türkiye adına gösterilebilecek örneklerdendir. Türkiye'de faaliyet yürüten İSS'lerden TTNNet, söz konusu Web sitesine erişimin engellenmesine ilişkin mahkeme kararı olmamasına rağmen, DNS hizmetinde kara liste uygulamak suretiyle kullanıcıların erişim taleplerine yanıt vermemektedir. İlgili hususta kontrollerin çevrimiçi olarak gerçekleştirilmesi mümkündür. Mahkeme kararına istinaden Erişim Sağlayıcıları Birliği tarafından erişimin engellenip engellenmediğine dair sorgulama için bkz 'Web Sitesi Erişim Engeli Sorgulama' (*Erişim Sağlayıcıları Birliği*) <<https://www.turkiye.gov.tr/esb-web-sitesi-erisim-engeli-sorgulama>> Erişim Tarihi: 05.02.2025. BTK tarafından uygulanan erişim engellerine dair sorgulama için bkz 'Site Bilgileri Sorgu Sayfası' (*BTK*) <<https://internet.btk.gov.tr/sitesorgu/>> Erişim Tarihi: 05.02.2025.

¹⁰¹ Zira uluslararası hukukun mevcut durumunda, faili elinde bulundurmeyen ve faile ait taşınmaz, banka hesabı vb. unsurlara da hâkim olmayan bir devletin, iade ve istinabe talep etmekten; talebine olumsuz karşılık aldığı anda ise failin bir şekilde "ağına düşmesini" beklemekten başka çaresi yoktur. *Post*, bu durumu çekiçle köstebek vurma oyununa benzetmiştir; David Post, 'Governing Cyberspace: Law' (2008) 24 Santa Clara High Technology Law Journal 883, 911.

III. MUKAYESE VE DEĞERLENDİRMELER

“Ağlar ağı” olan internet, farklı yapı ve amaçlara sahip yerel ve geniş alan ağlarını (*local area network (LAN) / wide area network-WAN*) bir araya getirerek bilginin sınır aşan biçimde eş zamanlı (*simultaneous*) ve gerçek zamanlı (*real-time*) iletimini sağlamaktadır. Böylece “küresel” nitelik kazanan internet üzerindeki devlet yetkilerinin, “uluslar-arası” nitelikte olan uluslararası hukuk hükümlerince tespit ve icrasında birtakım aksaklıklarla karşılaşılması kaçınılmaz olmuştur. Devletlerce başvurulmuş yöntemlerin temel sorunları; amaca uygunluk, etkililik, insan hak ve özgürlüklerine ve diğer devletlerin egemenlik alanlarına müdahale etmemeye dair üstlenilen uluslararası yükümlülüklerle uygunluk gibi başlıklarda gözlemlenmektedir. Sayılan başlıklar da birbirine çeşitli yönlerden etki etmekte, ideal denge noktasının bulunması yolunda ulusal ve uluslararası çabalar sürmektedir.

Gözetim ve denetim yönteminin etkililiği, sahip olunan teknik kapasiteye bağlıdır. Uluslararası hukuk açısından, devletin kendi ülkesinde gerçekleşen internet erişimi ile alınan/gönderilen paketleri izlemesi ve denetlemesi hususunda kural olarak bir engel bulunmamaktadır. Diğer yandan AIHS gibi sözleşmelerle kabul edilen yükümlülükler, devletlerin Avrupa İnsan Hakları Mahkemesi (AIHM) gibi uluslararası mahkemeler nezdinde yargılanmasına da kapı açmakta; bilhassa toplu gözetim uygulamaları, insan haklarına ilişkin uluslararası yükümlülükler bağlamında tartışılmaktadır.¹⁰² Uluslararası hukuk bakımından bir başka mesele ise devletlerin gözetim ve denetim faaliyetlerini ülke dışındaki kişilere yöneltmeleri halinde ortaya çıkmaktadır. Söz konusu faaliyetler, kullanıcıların ve ilgili ülkelere hâkim devletlerin rızaları dışında veya gizli tuttukları verilere yönelik gerçekleştiğinde ve ülkedeki siber unsurların işlevselliğine de bir müdahalede bulunulmadığı takdirde, uluslararası hukukun ihlal edilip edilmediği hususu tartışmalıdır.¹⁰³ Zira en ağır hali siber casusluk olarak kabul edilebilen bu tür faaliyetleri uluslararası hukukta yasaklayan bir normun yokluğu göze çarpmaktadır. Devletler, soruna çare olarak ulusal hukuklarında ihdas ettikleri düzenlemelerle diğer devletler tarafından icra edilmesi muhtemel veri gözetimi faaliyetlerinden korunmaya çalışmaktadır. Devlet otoritesinin kendi topraklarındaki münhasırlığının muhafazası bakımından, fiziksel zarara veya işlev kaybına neden olmasa dahi siber casusluk faaliyetlerinin, devlet egemenliğinin ihlali olarak kabul edilmesi gerektiği de öğretide ileri sürülmektedir.¹⁰⁴ Ülke dışındaki vatandaşların internet erişiminin gözetimi durumunda ise kişinin bulunduğu ülke devleti ile uyrukluğunda bulunduğu devletin mütedahil yetkisinden bahsedilebilecektir.

Gözetim ve denetime dair devlet tutumları incelendiğinde, farklı hukuk sistemlerine ve yönetim anlayışlarına sahip devletlerin, imkânlar elverdiğince söz konusu yöntemin icra zeminini genişletme girişimlerinde bulundukları görülmektedir. Bu uygulamalar, iletişimin ve

¹⁰² Emre Güzey, ‘AIHM Kararları Çerçevesinde Kitlelerin İstihbarat Maksatlı Gözetimi’ (2020) 30 SAVSAD Savunma ve Savaş Araştırmaları Dergisi 179, 198–200.

¹⁰³ Schmitt (n 65) 19–24 ve 170–174.

¹⁰⁴ Przemysław Roguski, ‘Violations of Territorial Sovereignty in Cyberspace—an Intrusion-Based Approach’ in Bibi van den Berg and Dennis Broeders (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020) 74.

özel hayatın gizliliğine yönelik eleştirilere sıklıkla konu olmaktadır. Ülke dışı gözetim faaliyetlerinin ise henüz mer'î uluslararası hukuka doğrudan aykırılığından bahsedilemese de devletler ve yazarlar nezdinde konuya ilişkin eleştiriler daha kuvvetli biçimde dile getirilmeye başlamıştır.¹⁰⁵

İçerik kaldırma, içeriğin bulunduğu sunucuya müdahale gerektirmesi yönüyle diğer yöntemlerden ayrılmaktadır. Devletin bir sunucuda bulunan içeriğin kaldırılmasını doğrudan sağlaması, ancak sunucuya yönelik gerçekleştireceği fiziksel müdahale veya uzaktan (*remote*) siber girişimle mümkün olacaktır. Doğrudan yönetim altında bulundurmadaıkları sunucular hakkında bu yöneme başvurmak, devletler bakımından büyük güçlük arz edecektir. Ayrıca böyle bir girişim, ülke dışındaki sunucuya yöneldiği takdirde; sunucudaki veri yapısı değişeceğinden işlev kaybına neden olunması hasebiyle, sunucuyu ülkesinde bulunduran devletin egemenliğinin ihlalinin bahsedilebilecektir.¹⁰⁶ Zira bir verinin sunucudan kaldırılması, akışının izlenmesine göre fiziksel yönü daha ağır basan bir süreçtir. Verilere nispetle sunucuların, ülke ve dolayısıyla devlet ile bağı da daha sıkıdır. Ancak çoğu durumda, sunucuyu ülkesinde bulunduran devletin, barındırılan veriyle menfaat ilişkisi zayıftır. Verinin internetteki mevcudiyetinde üçüncü devletlerin öncelikli menfaatleri de var olabilir. Doğal menfaat sahibi olan yer sağlayıcının ve ilgili site işletmecisinin tabiiyetinde bulunduğu devlet veya devletlerin de diplomatik koruma müessesesine gitmesi gündeme gelebilir. Bu nedenle devletler, ulusal hukuklarına aykırılık teşkil eden ve ülkeleri dışındaki sunucularda barındırılan içeriklerin kaldırılmasını hizmet sağlayıcılardan talep etmekte; taleplerine olumlu karşılık alamadıkları durumda ise ilgili devlet nezdinde hukuki girişimlerde bulunmakta yahut kendi ülkelerinde erişim engeli yöntemine başvurumaktadırlar.

Sunucuya nüfuz edilmesini gerektirdiğinden, bu çalışmada ele alınan yöntemler arasında ülke dışı uygulanması en güç seçenek içerik kaldırmadır. Sunucu ve içerik üzerinde yönetim yetkisine sahip kişilerin veya sunucunun ülke içinde bulunmaları durumunda ise süreç daha kolay işlemektedir. Bununla birlikte, hukuka aykırı içeriğin erişilemez hale gelmesi yolunda en etkin çözüm olarak kabul edilebilir. Ancak internetin yapısı gereği bilgi, büyük bir hızla ve neredeyse kontrolsüz biçimde yayılmaktadır. Bir içerik, bulunduğu sunucudan kaldırılabilse dahi sayısız farklı sunucuda kopyaları bulunmaya devam edebilmektedir. Dolayısıyla bu yöntem ancak etkili gözetim ve denetim faaliyetleriyle eşgüdüm içerisinde uygulandığı takdirde görece verimli sonuçlar elde edilebilmektedir.

¹⁰⁵ Dikkat çekici bir örnek olarak Rusya, BM bünyesindeki faaliyetler dahilinde sunduğu bilgilendirmede, ABD istihbaratının casus yazılımlarla sınır ötesinde gözetleme yapmasını; “Vaşington, uluslararası arenada kötü şöhretli ‘demokratik değerleri’ savunurken, uygulamada temel insan hak ve özgürlüklerinin korunmasını, BM Şartı’nı ve egemen eşitlik ile devletlerin iç işlerine karışmama gibi temel uluslararası hukuk ilkelerini açıkça ihmal etmektedir” ifadeleriyle yorumlamıştır; ‘On Spyware and Its Use by US Intelligence Services’ by Russian Federation (UN/Open-ended Working Group on Information and Communication Technologies 10 Temmuz 2024) Non-papers <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/Spyware_and_its_use_by_US_intelligence_services_ENG_0.pdf> Erişim Tarihi: 05.02.2025.

¹⁰⁶ Schmitt (n 65) 21.

Filtreleme ve erişim engeli, kullanıcıların internete erişebilmesi için İSS’lerden hizmet almasını zorunlu kılan ulusal hukuk düzenlemeleri ve internet mimarisi sayesinde, hukuka aykırı içeriğe karşı devletler bakımından en pratik ve uygulanabilir yöntemlerdir. Zira İSS’ler, hizmet verdikleri ülkede faaliyetlerini sürdürebilmek için devletlerden gelen talepleri uygulamak durumundadır.¹⁰⁷ Böylece yabancı Web sitesi ve uygulama işletmecileri de ilgili ülkedeki erişilebilirliğinin kısıtlanmaması adına genellikle devletlerle iş birliğine gitmeye yönelmektedir. Ülke dışındaki bir sunucuda barındırılan içeriğe veya sunulan hizmete erişimin ülke içinde engellenmesi de uluslararası hukuk açısından sorun doğurmamaktadır. Yöntemin zaafları ise yukarıda da değinildiği üzere gerek hizmet sağlayıcılar gerek kullanıcılar tarafından başvurulmuş çeşitli yollarla engel ve filtrelerin aşılabilmektedir. Diğer yandan, hukuka aykırı içeriğe erişim ülke içinde engellense dahi ülke dışında erişilebilir olmaya devam etmesi, bazı içerik türlerinde devletin veya vatandaşların menfaatlerine önemli zararlar verebilmektedir.

SONUÇ

Yukarıda ele alınan yöntemlerin işlerliğinin, devletlerin tutumlarına büyük ölçüde bağlı olduğu yadsınamaz. Ancak internetin küresel yapısıyla doğan sonuçların, ulusal hukuk normları ve uygulamaları vasıtasıyla kontrol altına alınmasındaki güçlük de aşıkardır. Hukuka aykırı içerikle mücadelede sıkça karşılaşılan “çekiçle köstebek vurma oyunu”, bir bakıma hukukun trajedisi gibi görünse de esasen titiz ve seçici işleyen, internet özgürlüğüne müdahalede ölçülü davranan hukuk sistemlerinde karşılaşılan bir olgudur. Oysa devletlerin, açık veya örtülü şekilde VPN hizmeti veren sunuculara erişimi engellemek, belirli yer sağlayıcıların sunucularına kapsamlı erişim engelleri getirmek, gözetim ve denetim uygulamalarını teknik olarak sıkılaştırmak; ileri seviyelerde, ülke içinde geniş çaplı internet kesintilerine gitmek ve hatta ülke dışına bağlantıyı keserek intranet uygulamasına dönmek gibi radikal seçenekleri de mevcuttur.

Mevcut haliyle internet, paydaşlarına büyük menfaatler sağlamaktadır. Ancak Türkçede “her nimetin bir külfeti vardır” ve “kar, zararın kardeşidir” gibi atasözleriyle kadim biçimde tasdik gördüğü üzere, zararlar da menfaatlerin yanında gelmektedir. Zararların hukuka aykırılık yönünün önüne geçmek, başta devletin görevidir. Nelerin zararlı, hukuka aykırı, milli güvenliği ve kamu düzenini tehdit edici vs. olduğunun tespitine ilişkin kabul edilen esaslar da devletten devlete değişebilmektedir. Bununla birlikte, *Svantesson*’un ifade ettiği gibi; “çoğu insan, internet araçlarının kendi ülkelerinin kanunlarına uymasını beklerken; muhtemelen internet araçlarının dünyadaki diğer tüm ülkelerin kanunlarına uymasını istemeyecektir”.¹⁰⁸ Çevrimiçi hizmetler ve internet içerikleri hakkında ulusal bazda alınan önlemlerdeki ve başvurulmuş yöntemlerdeki etkililik sorununun çözümünü yine ulusal hukuk normlarının ve icra araçlarının geliştirilmesinde aramak, ilk kertede makul ve gerekli görünmekle beraber; gerçekten

¹⁰⁷ Bkz n 94.

¹⁰⁸ Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017) 216.

amaçlanan noktaya ulaşabilmek için devletlerin uluslararası hukuk nezdinde iş birliğine gitmekten başka hukuki çözümlerinin bulunmadığı da anlaşılmaktadır.

Küresel olguların uluslararası girişimlerle düzenlenmesinde karşılaşılan siyasi, ekonomik, kültürel vs. gerekçelere dayalı zorluklar aşıkardır. Egemenlikle tavsif edilen devletler, bu vasıflarını sıkıca savunmaktadır. Sahip oldukları savunma refleksleriyle de hızla gelişen internetin kontrol altında tutulması yolunda önemli teknik kazanımlar elde etmiş; hukuki ve idari sistemlerini tekâmül ettirmişlerdir. Ancak tüm bu gidişat, internetteki hukuka aykırılığın önüne geçilmesinde ancak kısmi faydalar sağlamıştır. Zira devletin ülkesi ile sahip olduğu mutlak bağ ve sınırlılık durumu, internet için geçerli değildir.

İnternete ilişkin faaliyet gösteren şirketlerin, sınır ötesi hizmet sundukları devletlerin otoritelerine meydan okuyacak ölçüde teknik, ekonomik, sosyal ve kültürel iktidar sahibi olmaları, çoğu zaman ilgili devletlerin hukuku ve kamu düzeni adına ortaya çıkan sorunların nüvesi olarak kabul edilmekte; meseleler, devlet ve şirket arasındaki iktidar gerilimi üzerinden okunmaktadır. Oysa şirketleri tabiiyetinde bulunduran devletlerin de mevzubahis sorunların kaynağındaki ve çözümündeki konumları doğru değerlendirilmelidir. Zira böylece, şirket üzerinde tabiiyete binaen egemenliği bulunan devletin, diğer devletlerin egemenlik kaynaklı haklarına uygun sonuçlar doğuracak biçimde hareket etmesinin sağlanması zarureti anlaşılabacaktır. Söz konusu dengenin sağlanması adına halihazırda ulaşılabacak son adres ise uluslararası hukuktur. Devletler arasındaki iş birliği, asgari müşterekler düzeyinde dahi olsa güçlendirilerek; kapasite paylaşımı ile internet üzerinde yeni uluslararası denetleme ve icra mekanizmalarının kurulması, internetin küresel yapısından kaynaklanan zararların dikkate değer biçimde izalesini sağlayabilecektir. Devamında hizmet sağlayıcıların, ülkesel ve konum bazlı filtrelerle içeriklerini hizmet verdikleri ülkelerin ulusal hukuk sistemlerine uygun hale getirmesi; internet mimarisinin, hukukun gerektirdiği durumlarda kimlik tespitinin tamamen imkânsız hale gelmesinin önüne geçilecek şekilde kurgulanması; adli istinabe süreçlerinin işleyişinde uluslararası mutabakatın genişlemesi ve derinleşmesi; bilhassa çocukları korumak ve narkotik madde ticareti, insan ticareti, terörizm gibi suçları engellemek adına internet sükjeleri üzerinde etkin şekilde işleyecek bir sistemin uluslararası işbirliği ile tesis edilmesi yönündeki girişimler, devletlerin internet üzerindeki yetki icrasında karşılaşılan birçok soruna çözüm olacaktır. Nihai olarak, devletlerin ulusal çapta inşa ettikleri mekanizmaların ve başvurdukları yöntemlerin geldiği seviyeye rağmen; internetin özellikleri dikkate alındığında, hukukun işlerliğinin ve kamu düzeninin korunması adına uluslararası hukukun oynayacağı rol artık bir tercih değil zorunluluk olarak karşımıza çıkmaktadır.

KAYNAKÇA**Kitaplar, Kitap Bölümleri, Süreli Yayınlar ve Raporlar**

- American Civil Liberties Union, ‘Surveillance Under the USA/PATRIOT Act’ <<https://www.aclu.org/documents/surveillance-under-usapatriot-act>> Erişim Tarihi: 05.02.2025
- Arısoy MV and Küçüksille EU, ‘Performance Comparison of TOR Hidden Service Crawlers’ (2019) 6 Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi 147
- Baran P, ‘On Distributed Communications Networks’ (The RAND Corporation 1962) R-2626
- Berners-Lee T and Fischetti M, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor* (1st ed, HarperSanFrancisco 1999)
- Berners-Lee T, ‘Information Management: A Proposal’ (CERN 1989) <<https://cds.cern.ch/record/369245>> Erişim Tarihi: 05.02.2025
- Beyer JL, *Expect Us: Online Communities and Political Mobilization* (Oxford University Press 2014)
- Devon County Council, ‘Fire Beacons: Warning Signals Across the Countryside’ (2000) <<https://devoncc.sharepoint.com/sites/PublicDocs/Environment/Historic/Forms/AllItems.aspx?id=%2Fsites%2FPublicDocs%2FEnvironment%2FHistoric%2FSchools%2FFire%20Beacons%2Epdf&parent=%2Fsites%2FPublicDocs%2FEnvironment%2FHistoric%2FSchools&p=true&ga=1>> Erişim Tarihi: 05.02.2025
- Dixon M, *Textbook on International Law* (7th edn, Oxford University Press 2013)
- Farinho DS and Campos RR, ‘Models of Legal Liability for Social Networks: Between Germany and Portugal’ in Carlos Blanco de Moraes, Gilmar Ferreira Mendes and Thomas Vesting (eds), *The Rule of Law in Cyberspace* (Springer 2022)
- Fuchs C and others, ‘Introduction: Internet and Surveillance’ in Christian Fuchs and others (eds), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (1st edn, Routledge 2012)
- Griffiths J, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (2nd edn, Zed 2021)
- Güzey E, ‘AİHM Kararları Çerçevesinde Kitlelerin İstihbarat Maksatlı Gözetimi’ (2020) 30 SAVSAD Savunma ve Savaş Araştırmaları Dergisi 179
- Hauben R, ‘From the ARPANET to the Internet’ (23 Haziran 1998) <https://www.columbia.edu/~rh120/other/tcpdigest_paper.txt> Erişim Tarihi: 05.02.2025
- Hillier T, *Principles of Public International Law* (2nd edn, Cavendish Publishing 1999)
- Huyue Zhang A, *High Wire: How China Regulates Big Tech and Governs Its Economy* (Oxford University Press 2024)
- Kippenberger T, ‘How Did We Get to a World Wide Web?’ (1999) 4 The Antidote 21
- Korpisaari P, ‘From Delfi to Sanchez – When Can an Online Communication Platform Be Responsible for Third-Party Comments? An Analysis of the Practice of the ECtHR and Some Reflections on the Digital Services Act’ (2022) 14 Journal of Media Law 352

- Kuczerawy A, ‘From “Notice and Takedown” to “Notice and Stay Down”: Risks and Safeguards for Freedom of Expression’ in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020)
- Kumtepe CÇK, ‘Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliğinin Tallinn Rehberi Kapsamında Değerlendirilmesi’ (2022) 53 *The Turkish Yearbook of International Relations* 21
- Kurt SS, ‘Uluslararası Hukukta Diplomatik Koruma’ (2020) 6 *Anadolu Üniversitesi Hukuk Fakültesi Dergisi* 467
- Kurt T, ‘Panoptikondan Data Diktatörlüğüne: Özgürlüğün Sonu mu?’ (2023) 1 *Tokat Gaziosmanpaşa Üniversitesi Hukuk Fakültesi Dergisi* 137
- Lukasik S, ‘Why the Arpanet Was Built’ (2011) 33 *IEEE Annals of the History of Computing* 4
- Maheshwari S, McCabe D and Karni A, ‘House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App’ *The New York Times* (13 Mart 2024) <<https://www.nytimes.com/2024/03/13/technology/tiktok-ban-house-vote.html>> Erişim Tarihi: 05.02.2025
- Maréchal N, ‘Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy’ (2017) 5 *Media and Communication* 29
- Mueller ML, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (1. paperback ed, MIT Press 2004)
- Nojeim G, ‘FISA Court Opinion Outlines FBI Abuse of Key Intelligence Surveillance Authority’ (*Center for Democracy and Technology*, 4 Eylül 2020) <<https://cdt.org/insights/fisa-court-opinion-outlines-fbi-abuse-of-key-intelligence-surveillance-authority/>> Erişim Tarihi: 05.02.2025
- Öztekin A, *Teori ve Uygulamada Türk İnternet Hukuku* (1st edn, Seçkin Yayıncılık 2021)
- Pattenden P, ‘The Byzantine Early Warning System’ (1983) 53 *Byzantion* 258
- Post D, ‘Governing Cyberspace: Law’ (2008) 24 *Santa Clara High Technology Law Journal* 883
- Rada R, ‘Writing and Reading Hypertext: An Overview’ (1989) 40 *Journal of the American Society for Information Science* 164
- Richter A, ‘Regulation of Social Media in Russia’ (European Audiovisual Observatory 2021)
- Roguski P, ‘Violations of Territorial Sovereignty in Cyberspace—an Intrusion-Based Approach’ in Bibi van den Berg and Dennis Broeders (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020)
- Sanders K, ‘Fact-Checking John Oliver’s Interview with Edward Snowden about NSA Surveillance’ (*PolitiFact*) <<https://www.politifact.com/factchecks/2015/apr/09/edward-snowden/fact-checking-john-olivers-interview-edward-snowde/>> Erişim Tarihi: 05.02.2025
- Schiavetta S and Komaitis K, ‘ICANN’s Role in Controlling Information on the Internet’ (2003) 17 *International Review of Law, Computers & Technology* 267

- Schmitt MN (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)
- Shaw MN, *International Law* (8th edn, Cambridge University Press 2017)
- Soldatov A and Borogan I, 'Russia's Surveillance State' (2013) 30 World Policy Journal 23
- Staker C, 'Jurisdiction' in Malcolm D Evans (ed), *International Law* (4th edn, Oxford University Press 2014)
- Svantesson DJB, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press 2017)
- United Nations Open-ended Working Group on Information and Communication Technologies, 'On Spyware and Its Use by US Intelligence Services' by Russian Federation (2024) Non-papers <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_2021/Spyware_and_its_use_by_US_intelligence_services_ENG_0.pdf> Erişim Tarihi: 05.02.2025
- United States National Science Foundation, 'Birth of the Commercial Internet' <<https://new.nsf.gov/impacts/internet>> Erişim Tarihi: 05.02.2025
- United States House of Representatives, Judiciary Committee, 'USA Freedom Act' (*House Judiciary Committee Republicans*, 22 Nisan 2015) <<http://judiciary.house.gov/usa-freedom-act>> Erişim Tarihi: 05.02.2025
- Urban J and Quilter L, 'Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (2006) 22 Santa Clara High Technology Law Journal 621
- Wallace RMM and Martin-Ortega O, *International Law* (8th edn, Sweet & Maxwell 2016)

Ulusal Hukuk Düzenlemeleri

- Amerika Birleşik Devletleri, Amerikalıları Yabancı Hasım Kontrolündeki Uygulamalardan Koruma Yasası (*Protecting Americans from Foreign Adversary Controlled Applications Act*), 118th Congress, H.R.7521
- , Çocukların Çevrimiçi Mahremiyetinin Korunması Yasası (*Children's Online Privacy Protection Act*), 15 U.S. Code, §§6501-6506
- , Çocukların İnternette Korunması Yasası (*Children's Internet Protection Act*), 47 CFR 54.520
- , DARPA Kurucu Direktifi (*Department of Defence Advanced Research Projects Agency*), US Department of Defence, Directive 5105.15, 07.02.1958
- , Devletlerin ve Mağdurların Çevrimiçi Seks Ticaretiyle Mücadele Etmesine İzin Yasası (*Allow States and Victims to Fight Online Sex Trafficking Act*) ve Seks Tacirlerini Müsaadeyi Durdurma Yasası (*Stop Enabling Sex Traffickers Act*) (FOSTA-SESTA), 132 Stat. 1253 – Public Law No.115-164, 11.04.2018
- , Dijital Binyıl Telif Hakkı Yasası (*Digital Millennium Copyright Act*), 17 U.S. Code, §512
- , FISA Değişiklikleri (*FISA Amendments*), 129 Stat. 268 – Public Law No.114-23, 06.02.2015

- , Kolluk Kuvvetleri için İletişim Yardımı Yasası (*Communications Assistance for Law Enforcement Act*), Public Law 103-414
- , Sakıncalı İçeriklerin Özel Olarak Engellenmesi ve Filtrelenmesine Yönelik Koruma, (*Protection for Private Blocking and Screening of Offensive Material*), 47 U.S. Code, §230

Birleşik Krallık, Çevrimiçi Güvenlik Yasası 2023 (*Online Safety Act 2023*), Chapter.50

Çin Halk Cumhuriyeti Siber Güvenlik Yasası (*Cybersecurity Law of the People's Republic of China*), İngilizce Çeviri: <<https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>> Erişim Tarihi: 05.02.2025

—, Çevrimiçi Bilgi İçeriği Ekosisteminin Yönetişimine İlişkin Hükümler, Çin Siber Uzay İdaresi, 5 Numaralı Emir (*Provisions on the Governance of the Online Information Content Ecosystem, Order of the Cyberspace Administration of China No.5*), İngilizce Çeviri: <<https://wilmap.stanford.edu/entries/provisions-governance-online-information-content-ecosystem>> Erişim Tarihi: 05.02.2025

—, Çin Halk Cumhuriyeti Kriptografi Yasası (*Cryptography Law of the People's Republic of China*), İngilizce Çeviri: <<https://appinchina.co/government-documents/cryptography-law-of-the-peoples-republic-of-china/>> Erişim Tarihi: 05.02.2025

—, Kamu Güvenlik Kurumları Tarafından İnternet Güvenliği Gözetim ve Denetimine İlişkin Yönetmelik (*Regulations on Internet Security Supervision and Inspection by Public Security Bodies*), İngilizce Çeviri: <<https://digichina.stanford.edu/work/regulations-on-internet-security-supervision-and-inspection-by-public-security-bodies/>> Erişim Tarihi: 05.02.2025

Hindistan, 2000 Bilgi Teknolojisi Yasası (*The Information Technology Act, 2000*), Act No 21 of 2000.

Rusya Federasyonu, Bilgi, Bilgi Teknolojileri ve Bilginin Korunması Hakkında Federal Yasa (*Federal Law On Information, Information Technologies and Protection of Information*), The Russian Federation Federal law No. 149-FZ of 14 July 2006. <<https://eais.rkn.gov.ru/docs.eng/149.pdf>> Erişim Tarihi: 05.02.2025

—, Operasyonel Arama Faaliyetleri Federal Yasası (Federal Law on Operational-Search Activities), Federal Law No.144-FZ of 12 August 1995, <https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_373.pdf> Erişim Tarihi: 05.02.2025

Türkiye Cumhuriyeti, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, (RG 04.05.2007/26530)

—, 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanununda Değişiklik Yapılmasına Dair Kanun, (RG 26.04.2014/28983)

Web Sayfaları

BTK, 'Denetleme' <<https://www.btk.gov.tr/denetleme>> Erişim Tarihi: 05.02.2025

INHOPE, ‘Association of Internet Hotline Providers’ <<https://www.inhope.org/EN>> Erişim Tarihi: 05.02.2025

INTERPOL, ‘International Child Sexual Exploitation Database’ <<https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database>> Erişim Tarihi: 05.02.2025

IWF, ‘About Us’ <<https://www.iwf.org.uk/about-us/>> Erişim Tarihi: 05.02.2025

Instagram, ‘Kolluk Kuvvetlerine Yönelik Bilgiler’ <<https://help.instagram.com/494561080557017>> Erişim Tarihi: 05.02.2025

‘Türkiye: Uçtan Uca Şifreleme Korunmalı’ (*ARTICLE 19*, 20 Nisan 2023) <<https://www.article19.org/tr/resources/turkey-protect-end-to-end-encrypted-services/>> Erişim Tarihi: 05.02.2025

X, ‘Hukuki Talep SSS’ <<https://help.x.com/tr/rules-and-policies/x-legal-faqs>> Erişim Tarihi: 05.02.2025