GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 449-478
DOI: 10.17752/guvenlikstrtj.1708377

Derleme Makale
Review Article

Siber Güvenlik Kanunu'nun İletişim ve Yeni Medya Faaliyetleri Bağlamında Değerlendirmesi

Assessment of the Cybersecurity Law in the Context of Communication and New Media Activities

Mevlüt ALTINTOP*

* Doktora Öğrencisi, Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü, Gazetecilik Ana Bilim Dalı, Kayseri, Türkiye, e-posta: mevlutaltintop@hotmail.com, ORCID: 0000-0002-1731-9064

Geliş Tarihi / Submitted: 28.05.2025

Kabul Tarihi / Accepted: 03.11.2025

Öz

Yirmi birinci yüzyıl itibariyle büyük bir ivme yakalayan internet ve bilişim teknolojileri hayatın her alanını domine etmektedir. Sürecin ortaya çıkardığı dijitalleşme siyasi ve ekonomik işleyiş kadar iletişim süreçleri ve medya faaliyetleri ile gündelik hayat pratiklerinde de köklü değişimlere yol açmıştır. Bu değişimler yeni suç biçimlerinin ortaya çıkmasına ve güvenlik sorunlarına neden olmuştur. Devletler yasal düzenlemeler yoluyla bir yandan dijitalleşmenin neden olduğu bu suçları engellemeye çalışırken, diğer yandan da ortaya çıkan ihlal ve güvenlik sorunlarını aşmayı amaçlamaktadır. Sürecin en önemli parçalarından birisi internet ve bilişim teknolojileriyle desteklenen iletişim süreçleri ve yeni medya faaliyetleridir. Bu bağlama odaklanan çalışma, 12.03.2025 kabul tarihli ve 7545 numarasıyla 19.03.2025 tarihinde Resmî Gazete'de yayımlanan Siber Güvenlik Kanunu'nun iletişim ve medyayla ilgili bölümlerini Habermas'ın "Kamusal Alan" kavramsallaştırması ekseninde ele almaktadır. Yapılan analizlerde, Siber Güvenlik Kanunu'nun anayasal açıdan tanımlanmış ve güvence altına alınmış olan iletişim ve haberleşme özgürlüklerini kısıtlama, medya faaliyetlerini sınırlama getirme, yeterince şeffaf ve uyumlu olmaması nedeniyle keyfi uygulamalara yol açma gibi kamusal ve özel alana yönelik riskler taşıdığı sonucuna ulaşılmıştır.

Anahtar Kelimeler: Siber Güvenlik Kanunu, İletişim, Yeni Medya, Sosyal Medya, Sanal Dünya

Abstract

By the twenty-first century, the internet and information technologies, which have gained great momentum, dominate every aspect of life. The digitalization produced by this process has brought profound changes not only to political and economic operations but also to communication processes, media activities, and everyday practices. These changes have given rise to new forms of crime and security problems. States are attempting, through legal regulations, to prevent crimes caused by digitalization and to address security issues. One of the most important components of this process is the communication and new media activities supported by the internet and information technologies. This study examines the sections of the Cybersecurity Law related to communication and media within the framework of Habermas's conceptualization of the "public sphere"; the law was adopted on 12 March 2025 (Law No. 7545) and published in the Official Gazette of the Republic of Türkiye on 19 March 2025. The assessment concludes that the Cybersecurity Law poses risks of restricting constitutionally defined freedoms of communication and correspondence, imposing limitations on media activities, and–due to insufficient transparency and lack of coherence–leading to arbitrary application.

Keywords: Cybersecurity Law, Communication, New Media, Social Media, Virtual World

Extended Summary

This study critically evaluates the implications of Türkiye's Cybersecurity Law (Law No. 7545), enacted on March 19, 2025, by focusing on its impact on communication freedoms, media activities, and constitutional rights. The analysis emphasizes the tension between national security objectives and the protection of fundamental liberties in the digital age. The research employs a multidisciplinary approach, combining legal, sociological, and communication theories to assess the law's compliance with democratic principles and international human rights standards. The rapid digitalization of the 21st century has transformed political, economic, and social dynamics and has introduced new forms of crime and security challenges. States respond through legal frameworks like Türkiye's Cybersecurity Law, which aims to counter cyber threats but risks undermining constitutional rights. This study examines the law's provisions related to communication and media and argues that its vague language and broad enforcement powers threaten transparency, press freedom, and privacy.

The literature on cybersecurity is divided into technical studies, such as infrastructure security, and social science-oriented research, which addresses societal impacts. While technical studies dominate literature, few of them address the intersection of cybersecurity with communication and media. Key findings from prior work include the emphasis of international organizations like the North Atlantic Treaty Organization (NATO) and the European Union (EU) on transparency and human rights in cybersecurity policies and Türkiye's historically lagging legal infrastructure, exemplified by the 1991 "Crimes in the Field of Informatics", and low cybersecurity literacy among citizens, as shown in studies on university students. This study identifies a gap in research linking cybersecurity laws to communication freedoms and positions itself to fill this void.

Cybersecurity is defined as practices protecting digital systems, data, and infrastructure from threats, extending to societal and international dimensions. The term "cyber" originates from "cybernetics", reflecting control systems in digital environments. Cybercrime encompasses activities like hacking, data theft, and online harassment, requiring adaptive legal responses. The study highlights how communication has evolved beyond interpersonal exchanges to include systemic data transfers, network security, and digital infrastructure. This shift makes communication a critical component of national security strategies, as seen in Türkiye's Cybersecurity Law.

The law's provisions are analyzed in light of Türkiye's Constitution and international treaties such as the European Convention on Human Rights (ECHR) and International Covenant on Civil and Political Rights (ICCPR). Key findings include restrictions on fundamental rights, such as Article 13 of the law limiting freedom of expression by prohibiting media from disclosing information obtained by the Cybersecurity Presidency, and Article 6 granting authorities unchecked access to "log records", risking mass surveillance. Article 12 imposes broad media bans, contradicting democratic norms of proportionality and necessity. Ambiguities in the law, such as data retention policies lacking independent oversight and international data sharing without clear safeguards, raise concerns about misuse. Remote intervention powers in Article 6(1c) permit authorities to access communication infrastructure, threatening systemic transparency. The law diverges from EU and NATO guidelines, which prioritize human rights and judicial oversight, as seen in the absence of the ECHR's "necessary in a democratic society" criterion in Türkiye's implementation.

The study critiques the law's failure to balance security and freedom. Surveillance overreach through log collection and data centralization echoes Baudrillard's critique of virtual worlds replicating real-world power imbalances. Broad media bans and vague definitions of "cyber threats" may stifle dissent and undermine democratic discourse. Bureaucratic inertia in updating laws exacerbates rights violations, as seen in delayed responses to cybercrimes. To mitigate risks, this study proposes strengthening proportionality by aligning restrictions with constitutional principles, enhancing transparency through independent audits, adopting international norms like EU frameworks, and promoting digital literacy through public campaigns.

While the Cybersecurity Law addresses critical gaps in Türkiye's cyber defense, its ambiguous provisions and lack of safeguards endanger constitutional rights. This study underscores the need for reforms to reconcile security imperatives with democratic freedoms, urging policymakers to prioritize transparency, accountability, and international cooperation. Future research should explore the law's societal impact through qualitative studies and assess emerging technologies like Artificial Intelligence (AI) in cybersecurity frameworks.

Giriş

Yirmi birinci yüzyılla birlikte internet ve bilişim teknolojilerinin toplumsal yaşamdaki yaygınlığı keskin bir biçimde artarak siyasal, ekonomik, sosyal ve kültürel pratiklerinin yeniden düzenlenmesine yol açmıştır. Bu teknolojik dönüşüm, bilgi üretimi ve dağıtımının ötesinde kamusal tartışmanın biçimini, iletişim süreçlerini, medya faaliyetlerini ve bireylerin gündelik yaşam pratikleri de dönüştürmüştür. Değişim ve dönüşümün hayata birçok olumlu yansıması olmuştur fakat beraberinde olumsuz durumlar ve sorunlar getirmiştir. Bu bağlamda, örneğin, dijitalleşme yeni suç tipleri ve sistemik güvenlik riskleri doğurmuştur. Bu durum ise devletleri teknik tedbirler almanın yanında geniş ve kapsamlı yasal düzenlemeler yapmaya zorlamıştır. Onlardan biri olan ve bu çalışmanın odaklandığı 7545 sayılı Siber Güvenlik Kanunu[1], 12 Mart 2025'te kabul edilmiş ve 19 Mart 2025 tarihli Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

Çalışmanın temel amacı, Siber Güvenlik Kanunu'nun iletişim süreçleri ve yeni medya faaliyetleri üzerindeki doğrudan ve dolaylı etkilerini Jurgen Habermas'ın "Kamusal Alan" kavramı çerçevesinde analiz etmektir. Habermasçı perspektif, kamusal alanı rasyonel-kritik tartışmanın mekânı ve demokratik meşruiyetin nesnesi olarak ele almaktadır. Dolayısıyla ifade serbestliği, bilgiye erişim ve medya özerkliği gibi ölçütler, bu değerlendirme için normatif bir çerçeve sunmaktadır. Derleme makalesi olarak hazırlanan çalışma, metodolojik açıdan kanun metni ve ilgili düzenleyici belgelerin doküman incelemesine dayanmaktadır. Bu bağlamda "Kanun" hükümlerinin anayasal haklar, uluslararası sözleşmelerin dikkat çektiği insan hakları standartları ve uygulama mekanizmalarıyla ilişkisinin eleştirel bir yorumunu sunmaktadır.

İki blok üzerinde yapılan analizin ilkinde, Kanun'un ifade ve haberleşme özgürlükleri bakımından taşıdığı sınırlama riskleri, şeffaflık ve hesap verebilirlik ekseninde Anayasal hak ve özgürlükler ile uluslararası sözleşmeler bağlamında ele alınmaktadır. İkincisinde ise, Kanun'un teknik hükümlerde öngördüğü veri toplama, iletişim izleme ve müdahale yetkilerinin medya kuruluşlarının haber alma, haber üretme ve yayımlama süreçleri üzerinde baskı oluşturma potansiyeli tartışılmaktadır. Bir başka ifadeyle, her iki sürecin kamusal alan açısından ne anlama geldiği çözümlenmeye çalışılmıştır.

1 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*, Kanun No. 7545, 12 Mart 2025, https://resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm, erişim 13.05.2025.

Son olarak çalışma, Habermasçı normlar ile uyumlu olacak şekilde denetim mekanizmalarının güçlendirilmesi, orantılılık ilkesi ile teknik önlemlerin sınırlandırılması ve şeffaflık yükümlülüklerinin netleştirilmesi yönünde politika önerileri üretmeyi hedeflemektedir. Bu yaklaşım, hem hukuki meşruiyeti hem de kamusal tartışmanın demokratik niteliğini korumaya dönük bir normatif çerçeve sunarak, siber güvenlik konusunda iletişim süreçleri ve medya faaliyetleri bağlamında literatüre katkı sunmayı amaçlamaktadır.

1. Çalışmanın Amacı, Önemi ve Yöntemi

Çalışmanın amacını genel ve özel olarak iki aşamada açıklamak mümkündür. Çalışmanın genel amacı, günümüz dünyasının önemli unsurlarından olan siber ve siber güvenlik kavramlarına dikkat çekerek bu kavramlarının anlaşılmasına katkı sağlamak ve bu alandaki farkındalığı artırmaktır. Özel amacı ise, siber ve siber güvenlik kavramlarından yola çıkılarak oluşturulan yasal düzenlemenin bireysel, toplumsal ve kurumsal boyutlarının iletişim ve medya açısından anlamsal karşılığını bulmaya çalışmaktır.

Çalışmanın önemi, dijitalleşmenin büyük bir hızla artışının birey, toplum, kurum ve devletler açısından ortaya çıkardığı hayati sorunlardan kaynaklanmaktadır. İnternet ve bilişim teknolojileri aracılığıyla gerçekleştirilen zararlı faaliyetler, kişisel verilerin çalınması, finansal kayıplar ve hem ulusal hem de uluslararası güvenlik tehditleri (terör, casusluk vb.) açısından ciddi sonuçlara yol açabilmektedir. Sorun ve tehditleri bertaraf etmek için oluşturulan siber güvenlik önlemlerini almak, dijital ve ekonomik varlıkların korunması açısından kritik bir zorunluluktur. Bu çerçeve çalışmanın önemini de ifade etmektedir.

Derleme makalesi türünde yapılan bu çalışmada yöntem olarak doküman incelemesi kullanılmıştır. Bu bağlamda kitap, makale, kurum raporları, kanun maddeleri ve ilgili web sitelerinden faydalanılmıştır. Elde edilen inceleme sonuçları kapsamında, 12.03.2025 tarihinde kabul edilen ve 7545 numarasıyla 19.03.2025 Resmî Gazete'de yayımlanan Siber Güvenlik Kanunu'nun iletişim ve (yeni) medya ile ilgili kısımları analiz edilerek konunun kapsamlı ve karşılaştırmalı şekilde ele alınması sağlanmıştır. Değerlendirmede konuyla ilgili birçok kuramsal yaklaşıma değinilmiştir fakat çalışmanın ana izleğini Habermas'ın "Kamusal Alan" kavramsallaştırması oluşturmaktadır.

2. Literatür Taraması ve Kavramsal Çerçeve

Literatüre bakıldığında son yıllarda siber güvenlik ile ilgili çok faza çalışma yapıldığı ve bu çalışmalarda konunun genel olarak iki kategoride ele alındığı görülmektedir. İlki, siber ve/veya siber güvenlik konusunun donanım ve yazılım boyutunun değerlendirildiği teknik/teknoloji içerikli çalışmalardır. Bilişim teknolojilerine yönelik detayların yer aldığı bu çalışmalar siber teknolojilerinin mühendislik faaliyetleriyle ilgilidir. İkincisi ise, bu çalışmanın da dâhil olduğu, siber güvenlik konusunun kamusal ve toplumsal yansımalarına ele alan sosyal bilim ağırlıklı çalışmalardır. Bu çalışmalarda, siber teknolojilerin ulusal ve uluslararası olmak üzere iki kategoride çözülmesi gereken sorunlara yol açan gelişmeler olarak değerlendirildiği görülmektedir. Başka bir deyişle, siber teknolojilerinin yol açtığı siber güvenlik meselesi hem saldırı ve savunma, hem de asayiş sorunları olarak karşımıza çıkmaktadır. Öte yandan günümüz dünyasında teknik disiplinler ve teknolojik gelişmeler ideolojik bir form verilerek "sosyal mühendislik" faaliyetlerinde kullanılmaktadır.[2] Bu bağlamda, yukarıda değinilen ilk kategorinin de dolaylı olarak sosyal bilim alanıyla ilişkilendirilmesi mümkündür. Dolayısıyla siber teknolojilerin ulusal ve uluslararası alandaki etkisi ve bu etkinin toplumsal yansımasının bu yönü ayrıca dikkate alınmalıdır.

2 Nilüfer Göle, *Mühendisler ve İdeoloji* (Çev. Eli Levi), İletişim Yayınları, İstanbul, 1986, s. 13.

Konunun saldırı ve savunma bağlamı ülkelerin istihbarat ve askeri birimleri, silah sanayisi, enerji kaynakları ve ekonomik varlıklarına yönelik siber ortamda yapılan müdahaleleri konu edinmektedir. Bu alana dair yapılan çalışmalar ise genel olarak üç başlıkta toplanmaktadır. İlki, uluslararası bir sorun olarak siber güvenlik, ikincisi ulusal bir sorun olarak siber güvenlik ve üçüncüsü siber güvenliğe yönelik faaliyetlerin kamusal ve sosyal açılardan niteliğidir. Aşağıda bu üç başlığa dair örnekler verilerek çalışmanın ana izleği olan Siber Güvenlik Kanunu'nun iletişim süreçleri ve medya faaliyetleri açısından analizi yapılmıştır. Analizin temel argümantasyonunu Jurgen Habermas'ın "Kamusal Alan" kavramlaştırması oluşturmaktadır.

Tarihsel açıdan siber güvenlikte dönüm noktalarından biri, ABD'nin 1969'da ARPANET'i kullanmaya başlamasıdır. Başlangıçta askeri amaçlı olan bu sistem, veri paylaşımı ve iş birliği sağlayan bir dijital ortam olarak gelişerek günümüz internetinin temelini oluşturmuştur. Ancak internetin yaygınlaşmasıyla veri güvenliği riski de artmıştır.[3] Bilişim teknolojilerinin temel işlevleri (bilgiyi kaydetme, depolama, erişim sağlama ve işleme vb.) ihlal edildiğinde siber güvenlik sorunu ortaya çıkmaktadır.[4]

Siber dünya da tıpkı gerçek dünyada olduğu gibi hayatın olumlu ve olumsuz yönlerini yansıtmaktadır. Gerçek dünyada suç kelimesi en basit şekliyle, yetkili otoritenin belirlediği sınırların aşılması olarak tanımlanırken[5], siber dünyada ise bu durum "siber suç" olarak kavramsallaştırılmıştır.[6] Bununla birlikte, siber suçların kapsamı teknolojinin gelişimine paralel olarak genişlemektedir.[7] Bilişim teknolojilerinin mekân ve zaman kısıtlarını ortadan kaldırması, faaliyetlerin ulusal sınırları aşarak uluslararası boyut kazanmasına yol açmaktadır. Bu çerçevede, küresel normlar ve diplomatik yöntemler geliştirme çabaları gündeme gelmiştir.[8] Birleşmiş Milletler (BM), Avrupa Birliği (AB) ve Kuzey Atlantik Antlaşması Örgütü (NATO) gibi kuruluşlar da uluslararası sözleşmelerle bu alana müdahil olmaktadır.[9] Tüm bunlar siber güvenlik konusunu ulusal ve uluslararası bir boyuta taşımaktadır.

Batı'da 1990'larla birlikte toplumda karşılık bulan internetin Türkiye'de yaygınlaşması 2000'li yıllara denk gelmiştir.[10] Gecikmeye rağmen, Türkiye'de pek alışılmamış şekilde, bu alandaki yasal düzenlemeye dair faaliyetlerin daha önce başladığı görülmektedir. Örneğin 1991 yılında "Bilişim Alanında Suçlar"[11] başlıklı ilk yasal düzenleme yapılmış,[12] ancak

3 H. Alpay Karasoy ve Pelin Babaoğlu, "Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı", *Yasama Dergisi,* 44, 2021, s. 131.

4 Enes Çınar, *"Bilişim Suçları"*, Çınar Hukuk Bürosu, 2025, s. 2, https://www.cinarhukukburosu.com/blog/bilisim-suclari, erişim 11.05.2025.

5 Türk Dil Derneği, Türkçe Sözlük, Türk Dil Derneği, Ankara, 2012, s. 1576.

6 Çınar, "Bilişim Suçları", s. 20.

7 Zeynep Ata, "Sosyal Medyada Suç Korkusunun Oluşması ve Yayılması: X Örneği", *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 37, 2024, s. 395.

8 Tuba Eldem, "Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik", *İstanbul Hukuk Mecmuası*, 79:1, 2021, s. 349.

9 Sena Nezgitli ve Recep Benzer, "Avrupa Birliği Siber Güvenlik Kanunu", *Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi,* 2:1, 2020, s. 10.; Gülşah Özdemir, "Uluslararası Güvenlikte Siber Tehditlerin Yükselişi ve Stratejik Savunma Politikaları", *Elektronik Sosyal Bilimler Dergisi*, 24:1, 2025, s. 2-3.

10 Mevlüt Altıntop, *Zygmunt Bauman Sosyolojisinde İletişim Olgusu*, Kitapyurdu Doğrudan Yayıncılık, İstanbul, 2021, s. 76.

11 "Mülga 1926 tarih 657 sayılı Türk Ceza Kanunun Yürürlükten Kaldırılmış Hükümleri": Türk Ceza Kanunun Yürürlükten Kaldırılmış Hükümleri, 767 Mülga 765 sayılı Türk Ceza Kanunu On Birinci Bab Bilişim Suçları §§ 106-122, 1991, https://mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf, erişim 15.05.2025. Onbirinci Bap'ın dipnotunda şu ifadeler yer almaktadır: "Bu bap ve başlık, 6/6/1991 tarih ve 3756 sayılı Kanunun 20'nci maddesiyle metne eklenmiştir" "Mülga" kelimesinin sözlükteki karşılığı "kaldırılmış" şeklindedir. Türk Dil Derneği, *Türkçe Sözlük*, s. 1248.

12 Salih Bıçakçı, Doruk Ergun ve Mitat Çelikpala, *Türkiye'de Siber Güvenlik*, EDAM Siber Politika Kağıtları Serisi 2015/1, Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM), 25 Aralık 2015, s. 4, https://edam.org.tr/wp-content/uploads/2015/12/EDAM_TR_Siber_Guv_1.pdf, erişim 16.05.2025.

sonraki yıllarda mevzuat yetersiz kalmakla birlikte geçerli şekilde güncellenememiştir.[13] Bu konuda son yıllarda önemli ilerlemeler sağlansa da kaynak, eğitim ve şeffaflık gibi unsurlarda eksiklikler devam etmektedir.[14] 2003'ten bu yana sekiz eylem planı hazırlanmış[15] ve alanla ilgili kamusal kurumlar oluşturulmuştur.[16] Ancak teknolojiye hızla uyum sağlayan toplum karşısında, siyasi ve bürokratik yapıların geriden gelmesi, yasal boşlukların siber suçlular tarafından istismar edilmesine yol açmaktadır.[17]

Siber güvenlik konusunun iletişim süreçleri ve medya faaliyetleri boyutu literatürde sınırlı yer bulmaktadır. Mevcut çalışmalar genellikle teknik altyapıya odaklanmakta[18] ya da siber güvenlik konusundaki toplumsal farkındalığı ölçmektedir. Örneğin bu konuda yapılan az sayıdaki çalışmanın birinde iletişim fakültesi öğrencilerinin siber güvenlik ile ilgili farkındalık düzeyinin düşük olduğu saptanmıştır.[19] Bir başka ifadeyle, siber güvenlik ile ilgili yasal düzenlemelerin iletişim süreçleri ve medya faaliyetleri açısından anayasal düzlemle ele alan araştırmalar -yasal düzenlemelerle doğru orantılı olarak- son derece azdır. Çalışma bu bağlamda literatüre önemli bir katkı sunmayı amaçlamaktadır. Aşağıda öncelikle Habermas'ın Kamusal Alan yaklaşımı açıklanmış, ardından siber ve siber güvenlik literatürüne değinilmiş ve son olarak da yasal zemin açısından öncesi ve sonrasıyla Siber Güvenlik Kanunu değerlendirilmiştir.

2.1. Habermas'ın Kamusal Alan Yaklaşımı

Jürgen Habermas'ın kamusal alan kavramsallaştırması, modern demokratik toplumların iletişimsel yapısını anlamak açısından temel bir kuramsal çerçeve sunmaktadır. Habermas, ideal kamusal alanı, bireylerin kamusal meseleleri tartışmak, fikir alışverişinde bulunmak ve politik irade oluşturmak amacıyla bir araya geldikleri, devlet ve sermaye baskılarından görece bağımsız bir sosyal alan olarak tanımlamaktadır.[20] Bu alan, özellikle on sekizinci yüzyıl Avrupa'sında kafe, salon ve basın aracılığıyla gelişerek rasyonel-eleştirel tartışmaların demokratik meşruiyetin oluşumunda merkezi rol oynamasını sağlamıştır. Habermas'a göre, kamusal alanın ideal formu, katılımcıların eşitlik temelinde bir araya geldiği ve iletişimin güç ilişkilerinden arındığı bir ortamı gerektirmektedir.[21]

Habermas yirminci yüzyılda kamusal alanın yapısal dönüşüme uğradığını ileri sürmektedir. Yüzyılın ortalarında etkisi artıran kitle iletişim araçlarının zamanla daha fazla ticarileşmesi, kamusal söylemin giderek piyasa mantığı ve devlet propagandası tarafından şekillendirilmesine neden olarak rasyonel-eleştirel tartışma kültürünü zayıflatmıştır.[22] Bu durum, kamusal alanın demokratik işlevlerini yerine getirme kapasitesini azaltmakta ve

13 Hüseyin Çakır ve Murat Taşer, "Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi", *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji,* 11:2, 2023, s. 363.
14 Arzu Yıldırım, "Türkiye'nin Siber Güvenlik Politikasının Eylem Planları üzerinden Analizi", *Organizasyon ve Yönetim Bilimleri Dergisi,* 16:1, 2024, s. 23.
15 Karasoy ve Babaoğlu, *"Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı"*, s. 138.; Yıldırım, *"Türkiye'nin Siber Güvenlik Politikasının Eylem Planları üzerinden Analizi"*, s. 42.
16 Ali Burak Darıcılı, "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler", *TESAM Akademi Dergisi*, 6:2, 2019, s. 27-29.
17 Özen Akçakanat vd., "İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi", *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi*, 5:2, 2021, s. 267.
18 Muhammed Zekeriya Gündüz ve Resul Daş, "Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik", *Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 10:2, 2020, s. 971.
19 Mustafa Aksoğan vd., "İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği", *Kesit Akademi Dergisi*, 13, 2018, s. 285.
20 Jurgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Çev. Thomas Burger ve Frederick Lawrence), MIT Press, Cambridge, 1991.
21 Age, s. 56.
22 Age, s. 142.

yurttaşların politik katılımını pasifleştirmektedir. Habermas'ın teorisi, günümüzde dijital medya ortamlarının demokratik potansiyelini ve tehditlerini analiz etmek için de önemli bir referans noktası olarak kullanılmaktadır. Zira sosyal medya platformları hem yeni kamusal alan olanakları ortaya çıkarmakta, hem de popülizm, radikalizm, dezenformasyon, manipülasyon, propaganda ve kutuplaşma gibi kamusal alanın fayda eğilimi ortadan kaldırma risklerini beraberinde getirmektedir.[23] Buradaki en önemli detay, siber uzayın teoride sahip olduğu özgürlük ve demokratik katılım özelliği, Antik Yunan'daki kamusal alan olan agoranın postmodern versiyonu olarak değerlendirilmesidir. Bir başka ifadeyle, bugünün insanının ideal şartlarda hayatını sürdürebilmesi için sanal kamusal ("kamusanal") alana ihtiyacı vardır. Bu durum da, sanal kamusal ("kamusanal") alanda ortaya çıkan sorunların giderilmesini gerektirmektedir. Siber Güvenlik Kanunu da bunlardan sadece biridir.

2.2. Kavramsal Açıdan Siber ve Siber Güvenlik

"*Cybernetic*" sözcüğünün kısaltması olan "*cyber*" Türkçeye "siber" olarak çevrilmiştir ve "internete veya bilgisayara ait" anlamında kullanılmaktadır.[24] Daha geniş anlamıyla sibernetik, yapay veya biyolojik sistemlerin kontrol ve haberleşmesini konu alan bilim dalıdır. Etimolojik olarak Eski Yunancada "dümen tutan" anlamındaki *"kybernáō"*ya dayanmaktadır.[25] Siber kavramından türeyen "siber uzay" ise bilişim teknolojileri ve sanal ortamların oluşturduğu dijital evreni (siber uzayı) ifade etmektedir.[26]

Siber uzayda işlenen suçlara ilişkin farklı terimler bulunmakla birlikte, literatürde "siber suç" kavramı yaygın olarak benimsenmiştir.[27] Bu suçlar, bilişim sistemlerine izinsiz erişim, veri silme veya değiştirme gibi eylemleri ve ekonomik, ticari ya da siyasi amaçlı zarar/fayda ilişkilerini kapsamaktadır.[28] Bu bağlamda siber güvenlik, bilgisayar sistemlerini, ağları, yazılımları, kritik altyapıları ve verileri dijital tehditlerden koruma uygulamaları bütünü olarak kabul edilmektedir.[29] Bunun yanı sıra, uluslararası ilişkiler ve toplumsal süreçlerle de ilişkili olduğundan ulusal güvenlik boyutuna sahiptir.[30]

Siber kavramı, kontrol ve iletişim teorisinin kurucularından Norbert Wiener'in (1894-1964) *Cybernetics* adlı eserinde tanımladığı "geri besleme döngüleri"nden (*feedback loops*) türemiştir.[31] Dilimize teknik sistemlerin denetim süreçlerini betimleyen bir ön ek olarak

23 Jurgen Habermas, "Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension?", *Communication Theory,* 16:4, 2006, s. 420.

24 Türk Dil Kurumu, *Türkçe Sözlük*, 10. Baskı, Türk Dil Kurumu, Ankara, 2005, 2, s. 2093.

25 Sevan Nişanyan, *Nişanyan Sözlük Çağdaş Türkçenin Etimolojisi*, Liberus, İstanbul, 2022.

26 Mehmet Alperen Önal, "Siber Uzay Ve Güvenlik İlişkisi Bağlamında Siber Güvenliğin Boyutları", *Hitit Ekonomi ve Politika Dergisi*, 1:2, 2021, s. 115.

27 İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Adalet Yayınevi, Ankara, 2008, s. 13.

28 Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Suç Nedir?", Emniyet Genel Müdürlüğü (EGM), 2025, https://www.egm.gov.tr/siber/sibersucnedir? erişim 16.05.2025.

29 Soner Çelik, "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *ARHUSS,* 1: 2, 2018, s. 118.

30 Ulusal Siber Olaylara Müdahale Merkezi USOM, *Siber Güvenliğe İlişkin Temel Bilgiler*, Telekomünikasyon İletişim Başkanlığı, 2014, s. 1. https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf?, erişim 16.05.2025.

31 Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, 3. Baskı, MIT Press, Cambridge, 2019, s. 11. (İlgili kitap 1948 yılında yazılmış olup ikinci baskısı ise 1961 yılında yapılmıştır. Bu çalışmada 1961 yılında yapılan ikinci basımın 2019 yılında tıpkıbasım nüshası kullanılmıştır.) Geri besleme döngüleri (feedback loops), sibernetikte makinelerin veya organizmaların çevrelerine uyum sağlamasını ve denetimli davranış geliştirmesini açıklamak için kullanılan teknik bir terimdir. Sistem, çıktılara göre otomatik olarak kendini düzeltmek ya da geliştirmek için yeni girdi oluşturmaktadır. Bir başka ifadeyle sonuçlarına göre sistemin kendini veya eylemlerini kesme, sürdürme veya yeniden düzenleme sürecidir. Örneğin, bireyin sosyal medyadaki etkileşimin çokluğunun paylaşım yapmaya sevk etmesi veya sistemin beğenilere yönelik içerikleri kullanıcıya sunması geri besleme döngüleridir. Sibernetiğin kurucu ismi sayılan Wiener geri besleme döngülerini şöyle açıklamaktadır: *"(...) bir sistemin çıktısının, sistemin gelecekteki davranışını etkileyecek biçimde tekrar girdiye dönmesidir. Bu mekanizma, sistemin kendi davranışlarını düzenlemesini sağlar"*. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, s. 64.

geçmiştir.[32] Yirminci yüzyılın ortalarında Claude Shannon (1916-2001) ve Warren Weaver'ın (1894-1878) oluşturduğu Matematiksel İletişim Modeli'ndeki bilgi kuramı yaklaşımı, kanaldan geçen sinyallerin niceliksel ölçümünü vurgulayarak siber uzayın yalnızca devrelerden ibaret olmadığını ileri sürmektedir. Bu yaklaşım aynı zamanda belirsizlik ve gürültünün iletişimin ontolojik temellerinin birer parçası olduğunu savunmuştur.[33] Sosyal Sistemler Teorisi bağlamında Niklas Luhmann, sosyal ve teknik alt sistemlerin kendi kendini yeniden üreten bir ağ oluşturduğunu vurgulayarak internet dünyasının (siber uzayın) karmaşık uyum ve özerklik boyutlarını ortaya koymuştur.[34] Luciano Floridi'nin "bilgi etiği" perspektifi ise, "infosfer" kavramını benimseyerek dijital varlıkların etik statüsünün yalnızca araçsal değil aynı zamanda değer çerçevesinde ele alınması gerektiğini savunmaktadır.[35]

Ross Anderson'ın *Security Engineering* (Güvenlik Mühendisliği) adlı çalışmasında siber güvenlik olgusunu mühendislik, yönetişim ve hukuki düzenlemelerin kesişim noktasında yer alan disiplinler arası bir alan olarak tanımlanmaktadır.[36] Bruce Schneier ise şifreleme, güvenlik duvarları ve izinsiz giriş tespit sistemleri gibi teknik tedbirlerin yanı sıra risk yönetimi süreçlerinin de siber güvenliğin ayrılmaz parçası olduğunu belirtmektedir.[37] Bu kapsamda *National Institute of Standards and Technology* (NIST)'nin oluşturduğu çerçeve metinde kritik altyapı koruma standartları tanımlanarak, kuruluşların varlık envanteri, zafiyet değerlendirmesi ve olay müdahalesi süreçlerini sistematik hale getirmesi gerektiğini öngörmektedir.[38] Daniel Solove'un "Gizlilik Kuramı" ise kişisel verilerin sınıflandırılması ve kullanım senaryoları üzerinden mahremiyet ihlallerinin çok boyutlu analizine odaklanarak, siber güvenlik stratejilerinin "bireyin bilgi özerkliğini" de koruması gerektiğini ortaya koymaktadır.[39]

Siber suçlar alanında Ronald Clarke ve Derek Cornish, geleneksel suç tiplerinde görülen saldırgan tipolojileri, karar verme süreçleri ve eylemlerinin modellenerek dijital ortama uyarlanması gerektiğini ileri sürmüştür. Böylelikle geleneksel suç tipleri ve müeyyidelerinden hareketle dijital suç normlarının da oluşturulması ve/veya geliştirilmesi sağlanabilecektir.[40] David Wall ise siber suçları hem teknik saldırı yöntemleri hem de örgütlenme biçimleri bağlamında ele alarak, uluslararası iş birliğinin önemini ve sınır ötesi hukuki müesseselerin güçlendirilmesi gerektiğini vurgulamaktadır.[41] Konuyu "risk yönetimi" bağlamında ele alan Douglas Thomas ve Brian Loader, siber suç mücadelesinin etkinliğinin, güvenlik ve gözetim mekanizmalarıyla birlikte sivil özgürlüklerin korunmasına da bağlı olduğunu belirtmektedir.[42]

32 Nezir Akyeşilmen, *Disiplinlerarası Bir Yaklaşımla: Siber Politika & Siber Güvenlik*, Orion Kitabevi, Ankara, 2018, s. 54.
33 Claude E. Shannon, "A Mathematical Theory of Communication", *Bell System Technical Journal*, 27: 3, 1948, s. 379.
34 Niklas Luhmann, *Social Systems*, Stanford University Press, Stanford, 1996, s. 45.
35 Luciano Floridi, "Information Ethics: On the Philosophical Foundation of Computer Ethics", *Ethics and Information Technology*, 1, 1999, s. 42.
36 Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, New York, 2020, s. 3.
37 Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, Wiley, New York, 2004, s. 18.
38 Kevin M. Stine, Kim Quill, ve Gregory A. Witte, "Framework for Improving Critical Infrastructure Cybersecurity", *National Institute of Standards and Technology*, 2014, s. 5, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity, erişim 12.06.2025.
39 Daniel J. Solove, *Understanding Privacy*, Harvard University Press, Cambridge, 2007, s. 77.
40 Ronald V. Clarke ve Derek B. Cornish, "Modeling Offenders' Decisions: A Framework for Research and Policy", *Crime and Justice*, 6, 1985, s. 159.
41 David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge, 2007, s. 57.
42 Brian D. Loader ve Douglas Thomas, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age,* Routledge, London, 2000, s. 102.

Teknik boyutun ötesinde siber uzayın felsefi olarak ele alınması, Martin Heidegger (1889-1976)'in teknoloji eleştirisi özelindeki dünyakaynak ilişkisi analizine dayandırılabilir. Bu açıdan dijital platformlarda kullanıcı verilerinin "kaynak" hâline getirilmesi, modernitenin dayattığı araçsal bakışın bir tezahürüdür.[43] Michel Foucault (1926-1984) iktidarbilgi ilişkisine dayanan yaklaşımını oluştururken, modernitenin birey ve toplumu gözetim ve denetim altında tutma anlayışını açık olarak yansıtma özelliği nedeniyle Jeremy Bentham (1748-1832) tarafından geliştirilen bir hapishane modeli olan Panoptikon'dan faydalanmıştır.[44] Panoptikon metaforu dijital gözetim pratikleriyle (sinoptikon ve omniptikon)[45] örtüşmektedir ve siber güvenlik aktörlerinin veri toplama ve analiz faaliyetleri açısından iktidar olduğunu söylemek mümkündür. Bu bağlamda Gilles Deleuze (1925-1995) ve Félix Guattari'nin (1930-1992) "kontrol toplumları" eleştirisi ise sürekli izlenme ve veri profillemenin bireysel öznelliği otorite isteğine göre şekillendirdiğine dikkat çekmektedir.[46]

Bu bağlamda bir kontrol alanı olarak siber uzayda var olmaya çalışan bireyin kimlik ve öznellik yönlerinin etkilenme biçimleri üzerinde durulması gereken konulardandır. Tüm bu değerlendirmeler güvenlik ile teknolojinin iç içe geçen bir yapısı olduğunu göstermektedir ve böyle bir ortamda teknolojinin geldiği aşama güvenlik konusunun en önemli ayaklarından biri olan siber uzaydaki faaliyetleri oluşturmaktadır. Dolayısıyla bu ortamda güvenlik tesis edilirken herhangi bir suiistimal, ihlal, tehdit, risk ve zararlara karşı önlem almak başta devlet ve kurumları olmak üzere kamusal faydayı gözeten STK, akademi ve ekonomik kuruluşlara görevler düşmektedir.

Diğer yandan Manuel Castells'in "Ağ Toplumu" modelinde sosyal medya platformlarının demokratik katılım araçları açısından olumlu katkı sunduğunu fakat dezenformasyon ve manipülasyon bağlamında tam tersi bir etki yaptığı vurgulanmaktadır.[47] Hukuk felsefesi açısından en güncel tartışma metinlerinden biri olan Bir Adalet Teorisi (*A Theory of Justice*, 1971)'nde John Rawls'ın "adil ve eşit özgürlükler ilkesi ile adil fırsatlar ilkesi" kavramsallaştırmaları[48] bağlamında siber güvenlik düzenlemelerinin bireysel hakları koruyacak şekilde şekillendirilmesini, orantılılık ve demokratik denetim mekanizmalarının tesisini bir zorunluluk olduğunu söyleyebiliriz. Bu temel metinlere dayanan analitik çerçeve, Siber Güvenlik Kanunu'nun yeni medya ve iletişim faaliyetlerine ilişkin düzenlemelerini değerlendirirken iktidar, toplum, hukuk, güvenlik ve teknoloji ilişkisi ile bireysel haklar ve demokratik denetim mekanizmalarının birlikte ele alınmasının zorunluluğu ortaya çıkmaktadır. Yukarıdaki genel çerçeve bağlamında, çalışmanın ana izleği olarak seçilen Jurgen Habermas'ın İletişimsel Eylem Kuramı ile ilişkilendirdiği Kamusal Alan yaklaşımı, dijital kamusal alanda[49] şeffaf diyalog ve toplumsal uzlaşma için normatif bir çerçeve sunmaktadır.[50]

---

43 Martin Heidegger, *The Question Concerning Technology and Other Essays*, Harper & Row, New York 1977, s. 23.
44 Michel Foucault, *Hapishanenin Doğuşu* (Çev. Ali Yaşar Kılıçbay), İmge Kitabevi Yayınları, Ankara, 1992, s. 251.
45 Panoptikon, 360 derecelik görüş açısına sahip bir mimari yapı sayesinde tek kişinin birçok kişiyi aynı anda gözetleyebildiği "hapishane" modelidir. Sinoptikon, kitle iletişim araçları aracılığıyla çok sayıdaki kişinin az sayıdaki kişiyi gözetlediği ve/veya izlediği gündelik hayat pratiğidir. Omniptikon ise bilişim ve internet teknolojileri sayesinde çok sayıdaki kişinin gönüllü olarak çok sayıdaki kişiyi hem gözetlediği hem de onlar tarafından gözetlendiği etkileşimli bir işleyiştir. (Kaynak: Selin Bitirim Okmeydan, Postmodern Kültürde Gözetim Toplumunun Dönüşümü: 'Panoptikon'dan 'Sinoptikon' ve 'Omniptikon'a. *AJIT-e: Academic Journal of Information Technology*, 8: 30, s. 45.
46 Gilles Deleuze ve Félix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*, University of Minnesota Press, Minneapolis, 1987, s. 162.
47 Manuel Castells, *Ağ Toplumunun Yükselişi* (Çev. Ebru Kılıç), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2008, ss. 13-15.
48 John Rawls, *Bir Adalet Teorisi* (Çev. Vedat Ahsen Coşar), Phoenix Yayınevi, Ankara, 2017, s. 17.
49 Sanal kamusal alan olarak da tanımlanan dijital kamusal alan için ***"kamusanal alan"*** terkibi kullanılabilir.
50 Jurgen Habermas, *İletişimsel Eylem Kuramı* (Çev. Mustafa Tüzel), 1, Kabalcı Yayıncılık, İstanbul, 2001, s. 360.

Literatür taraması bağlamında temel bir kavramsal çerçeve çizildiğinde siber güvenlik literatürünün genel olarak üç ana eksende toplandığı görülmektedir. Bunlar, teknik altyapı odaklı çalışmalar, hukuki ve normatif çerçeveye odaklı çalışmalar ve yönetişim ve toplumsal etki analizleri şeklindedir. Aşağıdaki değerlendirme, buradaki üç başlıkta özetlenen sınıflandırma çerçevesinde ele alınarak Siber Güvenlik Kanunu'nun anayasal haklar ile iletişim ve medya özgürlüğü üzerindeki olası etkilerini anlamaya dönük metodolojik bir bağ kurmaktadır.

i. Teknik Yaklaşımlar

Bu grup çalışmalar, donanım ve yazılım güvenliği, ağ altyapısı, veri şifreleme, sızma testleri gibi mühendislik ve bilişim teknolojileri boyutlarını ele almaktadır.[51] Teknik araştırmalar, iletişim altyapısının korunmasında gerekli tedbirleri tanımlamaktadır. Ancak, çoğunlukla demokratik denetim, orantılılık ve ifade özgürlüğü gibi anayasal konulara değinmemektedir. Bu nedenle, hukuki analizler için yalnızca teknik çerçevenin yeterli olmadığı açıktır.

ii. Hukuki ve Normatif Çerçeve

Siber güvenliğin hukuki boyutuna odaklanan çalışmalar, ulusal mevzuatların gelişimi[52] ve uluslararası normların[53] anayasal ilkelerle uyumu konularını işlemektedir. Avrupa Birliği'nin Şebeke ve Bilgi Güvenliği Direktifi,[54] Budapeşte Konvansiyonu ve İkinci Ek Protokol[55] gibi belgeler, güvenlik önlemlerinin temel haklarla dengelenmesini öngörmektedir. Türkiye bağlamında ise 5651 sayılı Kanun,[56] Kişisel Verileri Koruma Kanunu (KVKK) ve Bilgi Teknolojileri İletişim Kurumu (BTK) düzenlemeleri,[57] Siber Güvenlik Kanunu öncesinde de dijital ortamda veri ve iletişim akışının kontrolünü mümkün kılan yetkiler sağlamaktadır. Ancak literatür, yeni kanunun önceki düzenlemeleri nasıl genişlettiği veya değiştirdiği konusunda sınırlı bilgi sunmaktadır.

iii. Yönetişim ve Toplumsal Etki

Toplumsal düzeyde yapılan araştırmalar, siber güvenlik politikalarının demokratik toplum ilkeleri, özgürlük-güvenlik dengesi ve ifade özgürlüğü üzerindeki etkilerini irdelemektedir.[58] Bu çalışmalar, siber güvenlik söyleminin gözetim teknolojilerini meşrulaştırma potansiyeline dikkat çekmektedir. Ancak literatüründe Siber Güvenlik Kanunu'nun özellikle iletişim süreçleri ve medya faaliyetlerinin dijital kamusal ("kamusanal") alan üzerindeki etkisini, anayasa hukuku perspektifinden ele alan kapsamlı bir değerlendirme bulunmamaktadır.

Mevcut literatür, teknik, hukuki ve yönetişim boyutlarında önemli birikim sunmakla birlikte, bu üç alanın iletişim süreçleri ve medya faaliyetleri bağlamında birbirine entegre

51 Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, s. 3; Schneier, *Secrets and Lies: Digital Security in a Networked World*, s. 18.

52 Karasoy ve Babaoğlu, *"Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı"*, s. 131.

53 Eldem, *"Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik"*, s. 371.

54 The Council of Europe, "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", The Council of Europe Publishing, Strasbourg, 2003, https://rm.coe.int/168008160f, erişim 10.05.2025.

55 The Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, The Council of Europe Publishing, Strasbourg, 2021.

56 Türkiye Büyük Millet Meclisi, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun No. 5651, 04 Mayıs 2007, https://resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm, erişim 15.05.2025.

57 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu*, Kanun No. 6698, 24 Mart 2016, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf, erişim 16.05.2025.

58 Ulrich Beck, *Risk Toplumu: Başka Bir Modernliğe Doğru* (Çev. Kazım Özdoğan ve Bülent Doğan), İthaki Yayınları, İstanbul, 2011, s. 232.; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2018, s. 119.

edildiği az sayıda çalışma mevcuttur. Tablo 1, bu konuda hem çalışmanın genel perspektifini hem de literatürdeki tematik sınıflandırmayı analitik sentez düzeyinde özet olarak sunmaktadır:

Tablo 1. Literatürde Tematik Sınıflandırma ve Analitik Sentez

Tema	Temel Kaynaklar	Literatürün Analitik/Kritik Sentezi
Hukuki Normatif Bağlam	*A Theory of Justice*,[59] *Understanding Privacy*,[60] Avrupa Konseyi Strasburg[61] ve Budapeşte Sözleşmeleri,[62] 5651 Sayılı Kanun,[63] 6698 sayılı KVKK,[64] Siber Güvenlik Kanunu.[65]	Bu literatür kümesi, temel haklar-özgürlükler ile güvenlik önlemlerinin meşruiyet koşullarını göstermektedir. Rawls'un öncelik ilkesi ve Solove'un mahremiyet sınıflandırması, veri-toplama ve ifade kısıtlarının hukukî sınırlarını ölçmek için kullanılabilme potansiyeline sahiptir. Uluslararası sözleşmeler ve ulusal kanunlar ise uygulamada hangi araçların meşru sayıldığına ilişkin normatif çerçeveyi sağlamaktadır.
Teknolojik Mühendislik Bağlamı	*Security Engineering*,[66] *Secrets and Lies*,[67] *Modern Operating Systems*,[68] *Framework for Improving Critical Infrastructure Cybersecurity*,[69] USOM/ BTK teknik rehberleri.[70]	Teknik literatür, loglama, olay müdahalesi, sistem bütünlüğü ve veri saklama uygulamalarının nasıl çalıştığını göstermektedir. Bu kaynaklar, hukuki kısıtlamaların pratikte uygulanabilirlik düzeyini ve teknik zorunlulukları anlamak için gereklidir.
Yönetişim Kurumsal Bağlamı	*Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı*,[71] *Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli* ***için Öneriler***,[72] BTK ve USOM resmi raporları,[73] AB Siber Güvenlik Strateji Belgesi.[74]	Kurumsal çalışmalar, hangi kurumların hangi yetkiye sahip olduğunu ve hesap verebilirliğin nasıl tesis edileceğini tartışmaktadır. Türkiye özelinde siber güvenlik ile ilgili resmî kurumların faaliyetlerinde yetki alanı, şeffaflık gibi kısımlarda belirsizlikler olduğu görülmektedir.

59 John Rawls, *A Theory of Justice*, Harvard University Press, Cambridge, 1971, s. 76.
60 Solove, *Understanding Privacy*.
61 Avrupa Konseyi, *"Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems"*.
62 Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*.
63 Türkiye Büyük Millet Meclisi, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.
64 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu*.
65 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.
66 Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*.
67 Schneier, *Secrets and Lies: Digital Security in a Networked World*.
68 Andrew S. Tanenbaum ve Herbert Bos, *Modern Operating Systems*, Pearson, New Jersey, 2015.
69 Stine, Quill ve Witte, *"Framework for Improving Critical Infrastructure Cybersecurity"*.
70 USOM, *Siber Güvenliğe İlişkin Temel Bilgiler*.
71 Karasoy ve Babaoğlu, *"Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı"*.
72 Darıcılı, *"Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler"*.
73 USOM, *Siber Güvenliğe İlişkin Temel Bilgiler*.
74 European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", *EDPS*, 2013, https://www.edps.europa.eu/sites/default/files/publication/13-06-14_cyber_security_en.pdf, erişim 19.05.2025.

İletişim ve Medya Etkileri Bağlamı	*The Theory of Communicative Action*,[75] Ağ Toplumunun Yükselişi,[76] *Convergence Culture*,[77] *The Age of Surveillance Capitalism*[78] kaynaklarındaki medya ile ilgili değerlendirmeler.	Bu kaynaklar dijital kamusal alanın yapısını açıklarken platform-dinamizmini, sosyo-kültürel dönüşümü, gözetim kapitalizminin yükselişini ve tüm bu gelişmelerin ifade ortamına etkisini ortaya koymaktadır. Kanundaki ifadeyi/erişimi sınırlayan hükümler buradaki değerlendirmelerin ortak tespiti olan demokratik açıdan olumsuz görüntüyle örtüşmektedir.

Çalışma, yukarıdaki sınıflandırmaya dayalı olarak Siber Güvenlik Kanunu'nu iletişim ve medya bağlamında spesifik biçimde ele alarak kapsamlı bir değerlendirme sunmaktadır. Ancak bu yaklaşım, kanunun multidisipliner yapısı nedeniyle genel çerçevesini bütünüyle yansıtamama riskini de beraberinde getirmektedir. Diğer yandan literatürde, özellikle siber güvenlik mevzuatının iletişim özgürlüğü, mahremiyet hakkı, orantılılık ve şeffaflık ilkeleri ile ilişkisini doğrudan tartışan ampirik ve normatif çalışmaların eksikliği göze çarpmaktadır. Bu eksikliği kısmen gidermeyi amaçlayan çalışma, kamusal alan ve siber güvenlik ekseninde ilerleyerek Siber Güvenlik Kanunu'nun iletişim süreçleri ve yeni medya faaliyetleri üzerindeki etkilerini incelemektedir. Ele alınan kavramsal çerçeve, teknik ve toplumsal boyutları kapsayan disiplinlerarası bir zeminde inşa edilmenin yanında, ana eksenini Habermas'ın "Kamusal Alan" yaklaşımı oluşturmaktadır. Kapsamın kısıtları gereği, yapılan değerlendirme anayasal açıdan bireysel haklar ve diğer hukuki düzenlemeler çerçevesinde iletişim ve medya alanındaki etkiler ile sınırlandırılmıştır. Bununla birlikte, literatür taraması ve kavramsal çerçeve bölümünde (iletişim süreçleri ve medya faaliyetlerinin kapsam dışında kalan) diğer alanlarla ilişkisine dair hususlara da kısmen değinilmiştir.

3. Siber Güvenlik Kanunu ve Öncesi

1990'ların sonlarından başlayarak dijital altyapıların yaygınlaşmasıyla Türkiye'de siber güvenlik alanı hem teknik hem kurumsal olarak gelişmiş, fakat idari ve yasal yetkiler uzun süreli bu evrim içinde parçalı bir gelişim göstermesi sonucu yetersiz kalmıştır. Bu dönemde yapılan düzenlemelere bakıldığında sorumluluk ve yetkiler, politika, koordinasyon, teknik müdahale, istihbarat ve adli/kolluk kurumlarının sorumlulukları arasında dağılım göstermiştir. Bunun yanında kişisel verilerin korunması ayrı bir yasal çerçeve altında düzenlenmiştir. Parçalı yapı ile görev ve yetki paylaşımının net tanımlanamaması kurumların faaliyetlerinde örtüşme/boşluk ve sürtüşmeler doğurmuştur. Sağlıklı işlemeyen bu yapı koordinasyon, etkin bilgi paylaşımı ve hukuki şeffaflık gereksinimlerini ön plana çıkarmıştır.[79] Siber Güvenlik Kanunu öncesinde Türkiye'de siber güvenlik ile ilgili yetkilendirilmiş çok parçalı yapı şöyledir.

i. Bilgi Teknolojileri ve İletişim Kurumu (BTK): BTK, elektronik haberleşme düzenleyicisi olarak yıllar içinde ulusal siber güvenlik politikalarının oluşturulmasında merkezi bir rol üstlenmiştir. BTK çatısı altında çalışan ve ülke çapında koordinasyonu sağlamaya yönelik mekanizmalar ile (Siber Güvenlik Kurulu vb.) strateji, politika ve kritik altyapı belirleme gibi görevler yerine getirilmiştir. Ayrıca düzenleyici/denetleyici yetkiler kapsamında erişim, telekomünikasyon altyapısı ve bazı güvenlik standartlarına ilişkin

75 Jurgen Habermas, *The Theory of Communicative Action* (Çev. Thomas McCarty), Beacon Press, Boston, 1984.
76 Castells, *Ağ Toplumunun Yükselişi*.
77 Henry Jenkins, *Convergence Culture: Where Old and New Media Collide*, New York University Press, New York, 2006.
78 Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.
79 Ege Çakırca, Tuna Çakırca ve Oylum Çelik, "Türkiye'de Siber Güvenliğin Yeni Yasal Çerçevesi: 7545 Sayılı Siber Güvenlik Kanunu", *Turkish Law Blog*, 16 Mayıs 2025, https://turkishlawblog.com/insights/detail/turkiyede-siber-guvenligin-yeni-yasal-cercevesi-7545-sayili-siber-guvenlik-kanunu, erişim 15.08.2025.

düzenlemeler yapma kapasitesine sahiptir. Bu yetkiler, ilgili elektronik haberleşme mevzuatı ve BTK'nin kurumsal düzenlemeleri temelinde kullanılmıştır.[80] Diğer yandan BTK'nin bilgi-belge talep etme yetkisi, sektörel düzenleme ve denetim çerçevesinde sınırlı, mevzuata bağlanmış ve idari yaptırımlara tabi bir yetki formu olarak ortaya çıkmaktadır. BTK, 5809 sayılı Elektronik Haberleşme Kanunu kapsamında bu alana ilişkin düzenleme, denetim ve denetim sonucu elde edilecek bilgi ve belgelerin talep edilmesi yetkisini kullanmakta ve mevzuata aykırılıklar halinde idari para cezası gibi yaptırımlar uygulayabilmektedir.[81]

ii. USOM / TR-CERT (Ulusal Siber Olaylara Müdahale Merkezi): Teknik müdahale, olay tespit-haberleşme ve ulusal tehdit paylaşımı fonksiyonları büyük oranda USOM (TR-CERT) çerçevesinde yürütülmüştür. USOM, 7/24 faaliyet gösteren bir ulusal CSIRT merkezi olarak kurumlar arası olay koordinasyonu, uyarı yayma, tehdit analizi ve kurumsal SOME'lerle eşgüdüm sorumluluğu üstlenmiştir. Operasyonel işleyişi BTK ile yakın ilişki içinde olan USOM'un uygulamaları, müdahale süreçleri ve kurumsal SOME (CSIRT) ağı, uygulamadaki teknik kapasitenin omurgasını teşkil etmiştir.[82]

iii. Millî İstihbarat Teşkilâtı (MİT) ile İçişleri Bakanlığı/Emniyet Genel Müdürlüğü: MİT, ulusal güvenlik boyutundaki (siber istihbarat, yabancı kaynaklı tehditler vb.) faaliyetler ve istihbarat toplama görevleriyle bu alanın güvenlik-istihbarat cephesini temsil etmektedir. İçişleri bakanlığına bağlı Emniyet Genel Müdürlüğü ise siber suç soruşturmaları, adli takip, kolluk operasyonları ve suç delillerine erişim süreçlerinde yetkili organlardır. Bu aktörlerin yetkileri, istihbarat ve kolluk hukukuna ilişkin ayrı mevzuat ile düzenlenmiş olup pratikte bilgi paylaşımı ve operasyonel koordinasyonunu BTK/USOM ile etkileşim hâlinde yürütmektedir.[83]

iv. KVKK ve Sektör Düzenleyicileri (BDDK, EPDK, SPK vb.): Kişisel verilerin korunması veri işleme süreçlerinin hukuki çerçevesini belirleyen kanun, sektör bazlı düzenleyiciler (örneğin bankacılık, enerji, sermaye piyasaları) kendi alanlarına münhasır ek düzenlemeler ve yükümlülükler koyabilme yetkisi verilmiştir.[84] Bu iki katmanlı düzenleme, veri koruma ile siber güvenlik tedbirleri arasında hem işbirliği hem de uyum gerektiren bir ilişkiyi getirmiştir fakat hem yetki alanı belirsizliği hem de çift başlılık doğurmuştur.

v. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO): CBDDO geleneksel olarak politik–stratejik koordinasyon, dijital dönüşüm politika ve rehberliği ile kamu kurumları arası eşgüdüm rolü üstlenen; doğrudan cezaî/idari yaptırım uygulama veya zorlayıcı belge/erişim talebi yetkisi olmayan bir yapıdır.[85] Ancak, 28 Mart 2025 tarihli Cumhurbaşkanlığı kararnamesiyle CBDDO kapatılmış[86] ve bazı görev ile yetkileri genişletilerek Siber

80 Bilgi Teknolojileri ve İletişim Kurumu, "Siber Güvenlik Kurulu", *Bilgi Teknolojileri ve İletişim Kurumu*, 2025, https://www.btk.tr/siber-guvenlik-kurulu, erişim 15.08.2025.

81 Türkiye Büyük Millet Meclisi, *Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği*, Yönetmelik No 28914, 2014, https://www.resmigazete.gov.tr/eskiler/2014/02/20140215-7.htm, erişim 15.08.2025; Türkiye Büyük Millet Meclisi, *Elektronik Haberleşme Kanunu*, Kanun No 5809, 05 Kasım 2008, https://resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm, erişim 15.05.2025.

82 Ulusal Siber Olaylara Müdahale Merkezi, "Hakkımızda/about Us", *Ulusal Siber Olaylara Müdahale Merkezi*, 15 Ağustos 2025, https://www.usom.gov.tr/hakkimizda, erişim 15.05.2025.

83 Millî İstihbarat Teşkilâtı, *"Yetki ve Sorumluluklar", Millî İstihbarat Teşkilâtı (MİT)*, 2025, https://www.mit.gov.tr/yetki-ve-sorumluluklar.html, erişim 15.08.2025; Siber Suçlarla Mücadele Daire Başkanlığı, *"Siber Suç Nedir?*".

84 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu*.

85 Govinsider, "Digital Transformation Office (DTO) of the Presidency of the Republic of Türkiye", *Govinsider*, 2025, https://govinsider.asia/intl-en/digital-government/country/turkey?utm_source=chatgpt.com&type=info&agency=digital-transformation-office-dto-of-the-presidency-of-the-republic-of-turkiye-80, erişim 15.08.2025.

86 Hüseyin Cem Dağıstanlı ve Abdullah Sarıca, "Cumhurbaşkanlığına bağlı ofis ve politika kurullarına ilişkin düzenlemeler Resmi Gazete'de", *Anadolu Ajansı*, 28 Mart 2025, https://www.aa.com.tr/tr/gundem/cumhurbaskanligina-bagli-ofis-ve-politika-kurullarina-iliskin-duzenlemeler-resmi-gazetede/3522186, erişim .

Güvenlik Başkanlığı veya ilgili yeni yapılar arasında yeniden dağıtılmıştır. Bu görev devri/organizasyon değişikliği sonucunda Siber Güvenlik Kanunu bağlamında başkanlığa tanınan "kurum ve kuruluşlardan bilgi ve belge talep etme" gibi geniş erişim yetkileri, CBDDO'nun daha çok koordinatif nitelikteki fonksiyonları ile BTK'nin sektörel, yaptırıma dayalı denetim yetkileri arasında hibrit bir yetki profilinin doğmasına yol açmıştır. Diğer bir deyişle, politik koordine edici roller ile zorlayıcı erişim-yetkilerinin aynı merkezde toplanması, hem hukuki sınırların yeniden çizilmesini hem de denetim ve hesap verebilirlik mekanizmalarının güçlendirilmesini gerektirmektedir.[87]

Yukarıdaki yetki ve uygulama aşamalarındaki sorunları gidermek amacıyla Siber Güvenlik Kanunu çıkarılmıştır. Daha geniş ifadeyle, bu Kanun'a duyulan ihtiyaç, Türkiye'de siber tehditlerin artan sıklığı ve karmaşıklığı karşısında mevcut mevzuatın dağınık ve yetersiz kalması; kritik altyapıların, kamu hizmetlerinin ve özel sektör veri varlıklarının etkin korunamaması; olaylara hızlı müdahale ve koordinasyon kapasitesinin güçlendirilmesinin gerekliliğinden kaynaklanmıştır (Kanun'un amaç ve kapsamı Resmî Gazete'de açıkça belirtilmiştir).[88] Ayrıca Kanun, siber olaylara ilişkin raporlama, sorumlulukların netleştirilmesi, ulusal strateji ve merkezî bir yönetim/başkanlık yapısının kurulması yoluyla hem önleme hem de müdahale mekanizmalarını hukuki zemine oturtmayı hedeflemektedir. Böylece kurumlar arası koordinasyon eksikliğini gidermeyi ve cezaî/idarî yaptırımlarla caydırıcılığı artırmayı amaçlamaktadır.[89] Bununla birlikte kritik sektörlerin korunması, yerli siber güvenlik ekosisteminin güçlendirilmesi ve uluslararası iş birliği ile bilgi paylaşımının düzenlenmesi ihtiyacına da cevap vermek amacıyla hem operasyonel hem de stratejik zafiyetleri kapatmayı amaçlayan kapsamlı bir düzenleme ihtiyacının sonucu olarak ortaya çıkmıştır.[90]

4. İletişim Süreçleri ve Medya Faaliyetleriyle İlgili Anayasal Hak ve Özgürlükler ile Uluslararası Sözleşmeler Bağlamında Siber Güvenlik Kanunu

Siber güvenlik ve hukuk arasındaki ilişki, dijitalleşen dünyada giderek daha karmaşık ve çok katmanlı bir hâl almıştır. Siber güvenlik, sadece teknik bir mesele olmaktan çıkıp, ulusal ve uluslararası hukuk sistemlerinin düzenleme ve müdahale alanına girmiştir. Bu bağlamda, siber güvenliğin sağlanması ve korunmasında hem ulusal hem de uluslararası hukuk düzenine önemli roller düşmektedir.[91] Siber alandaki faaliyetlerin düzenlenmesinde hukuk, geleneksel devlet hukukunun ötesine geçerek, farklı normatif düzenlemeleri ve kural koyucuları içeren çok hukuklu bir yapıya dönüşmektedir.[92] Bu durum, siber güvenlik alanında hukuki düzenlemelerin, teknolojik gelişmelerle eş zamanlı olarak evrilmesini ve adaptasyonunu zorunlu kılmaktadır. Ayrıca, siber suçların artması ve çeşitlenmesi, kamu otoritelerinin sorumluluğunu artırmakta ve bu alanda etkin hukuki mekanizmaların geliştirilmesini

87 Aslıhan Deniz Bilgehan, "Siber Güvenlik Başkanlığının Düzenlenişine Dair Değerlendirme", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 12:1, 2025, ss. 63-88,

88 Siber Güvenlik Kanunu, c. 7545.

89 Mehmet Karlı, Osman Gazi Güçlütürk ve Zeynep Ekinci, "Türkiye'de Siber Güvenlik Kanunu Yürürlüğe Girdi", *Lexology*, 20 Mart 2025, https://www.lexology.com/library/detail.aspx?g=ea84ee2a-52c2-4abe-acb1-2c48021f85cf, erişim 16.08.2025.

90 Gözde Esen Sakar, Ece Nart ve Pelinsu Üstündağ, "7545 Sayılı Siber Güvenlik Kanunu", *Mondaq*, 02 Nisan 2025, https://www.mondaq.com/turkey/security/1606732/7545-say%C4%B1l%C4%B1-siber-g%C3%BCvenlik-kanunu, erişim 15.08.2025.

91 Merve Erdem ve Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 68:1, 2019, s. 130.

92 Fatma Hatipoğlu Aydın, *Siber Güvenlik ve Kişisel Verilerin Korunması: Hukuki Bir Değerlendirme*, Adalet Yayınevi, Ankara, 2023, s. 50.

gerektirmektedir.[93] Sonuç olarak, siber güvenlik ve hukuk arasındaki ilişki, dinamik ve sürekli gelişen bir alan olup, etkin bir siber güvenlik stratejisi için hukuki altyapının güçlendirilmesi ve güncellenmesi elzemdir.

Dijitalleşen dünyada iletişim, yalnızca bireyler arası mesaj alışverişi olmaktan çıkarak, sistemler, kurumlar ve devletlerarasındaki ilişkileri kapsayan interaktif ve stratejik bir alana dönüşmüştür. Türkiye'de 2025 yılında yürürlüğe giren Siber Güvenlik Kanunu, siber uzayda kamu güvenliğini artırmayı hedeflerken, aynı zamanda iletişim sistemleri üzerinde ciddi etkiler oluşturmaktadır. Siber uzayın gelişimi, iletişim kavramını hem teorik hem pratik anlamda dönüştürmektedir. Devletlerin dijital ortamda birey, toplum ve kurumları korumaya yönelik çabaları, yalnızca teknik düzenlemeleri değil, aynı zamanda iletişim ve medyayı kontrol altına alma stratejilerini de içermektedir. Siber Güvenlik Kanunu bu bağlamda değerlendirildiğinde iletişim sosyolojisi, kitlesel medya çalışmaları, siyasal iletişim ve kültürel yapı açısından önemli düzenlemeler içerdiği görülmektedir. Aşağıda, bu düzenlemelerin son örneği olan Siber Güvenlik Kanunu, anayasal hak ve özgürlükler bağlamında analiz edilmiştir.

4.1. Anayasal Haklar ve İletişim Özgürlüğü Bağlamında Siber Güvenlik Kanunu'nun Değerlendirmesi

İletişim hakkı, demokratik toplumların temel unsurlarından biri olarak, bireylerin bilgi alma, yayma ve ifade özgürlüğünü kapsamaktadır.[94] Bu hak, yalnızca bireyler arası ilişkiyi değil, aynı zamanda kamusal alanın işleyişini ve siyasal katılım süreçlerini doğrudan etkilemektedir. Türkiye Cumhuriyeti Anayasası başta olmak üzere, tarihsel süreç içinde yürürlüğe giren Basın Kanunu, Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun ve İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun gibi yasal düzenlemeler bu alanı şekillendirmektedir. 2025 tarihli Siber Güvenlik Kanunu, bu yasal çerçeveye yeni bir katman ekleyerek dijital iletişim alanında ilgili resmî kurumlara güçlü müdahale yetkileri tanımlamaktadır. Tablo 2'de, Siber Güvenlik Kanunu kapsamında anayasal olarak bireyin iletişim ve medyaya ilişkin sahip olduğu haklara yer verilmiştir:

Tablo 2. Bireyin Anayasal Olarak Sahip Olduğu Haklar ve Siber Güvenlik Yasasıyla İlgili Bölümlerinin Değerlendirmesi

Madde	İçerik ve Açıklama	Değerlendirme
Anayasa'nın 26. Maddesi: İfade Özgürlüğü	Türkiye Cumhuriyeti Anayasası'nın 26. maddesi, herkesin düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla açıklama ve yayma hakkına sahip olduğunu belirtmektedir.[95] Siber Güvenlik Kanunu 13. maddesiyle, Başkanlık tarafından edinilen bilgi ve belgelerin medya aracılığıyla paylaşılmasını yasaklayarak bu özgürlüğü daraltmaktadır.[96] Bu durum, ifade özgürlüğü ile kamu güvenliği arasında anayasal bir denge sorununu gündeme getirmektedir.	İfade özgürlüğü, güvenlik gerekçesiyle ciddi biçimde sınırlanmakta; anayasal hak ile yasa arasında denge bozulmaktadır.

93 Ahmet Efe, *Bilişim Suçları ve Türk Ceza Hukukundaki Yeri*, Seçkin Yayıncılık, Ankara, 2017, s. 5.
94 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*, TBMM Basımevi, Ankara, 2020.
95 Age, s. 30.
96 Türkiye Büyük Millet Meclisi, "Siber Güvenlik *Kanunu"*, Kanun No. 7545, 12 Mart 2025, https://resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm., erişim: 12.06.2025.

Anayasa'nın 22. Maddesi: Haberleşme Hürriyeti	Anayasa'nın 22. maddesi, haberleşme hürriyetini güvence altına almaktadır.[97] Bu hak, yalnızca kişisel yazışmaları değil, internet üzerinden veri alışverişini ve dijital haberleşme süreçlerini de kapsamaktadır. Siber Güvenlik Kanunu'nun 6. maddesi, Başkanlık'a "log"[98] verileri toplama, inceleme ve saklama yetkisi verirken, bu hak üzerinde istisnai bir denetim yetkisi tanımaktadır.[99] İlgili maddenin, *"gerekli olduğu sürece"* verilerin saklanmasına izin vermesi, orantılılık ve ölçülülük ilkesi çerçevesinde tartışmalıdır.	Özel hayatın gizliliği ihlal etme ve keyfi veri toplama, denetim dışı uygulamalara kapı aralama riski taşımaktadır.
5187 Sayılı Basın Kanunu ve Yayın Özgürlüğü	5187 sayılı Basın Kanunu, basının serbestçe bilgi edinme, yayma ve eleştirme hakkını güvence altına almaktadır.[100] Ancak Siber Güvenlik Kanunu'nun 12. ve 13. maddelerinde getirilen yayın yasağı ve medya açıklama kısıtlamaları, bu özgürlüğü ciddi biçimde sınırlandırmaktadır. Özellikle "her türlü medya aracıyla açıklama yasağı"nın kapsamı oldukça geniş olması basın özgürlüğü ilkesiyle örtüşmemektedir.	Medya üzerindeki baskı artırılmıştır. Bu durum medyanın kamusal fayda sağlayıcı faaliyet yapma niteliğine zarar verebilme riski taşımaktadır.
5651 Sayılı Kanun ve İnternet Yayıncılığı	İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun (5651) internette içerik ve yer sağlayıcıların yükümlülüklerini belirlerken, içeriklerin kaldırılması ve erişimin engellenmesini de düzenlemektedir.[101] Siber Güvenlik Kanunu bu yapıya paralel olarak, bazı maddelerde 5651'i referans almakta ve hatta 19. maddede bu kanunda değişiklik yapmaktadır. Ancak Siber Güvenlik Kanunu, içeriğe değil sisteme dair erişim, kayıt ve gözetim yetkilerini tanımladığı için daha üst düzey bir denetim mekanizması inşa etmektedir.	İçeriklerin kontrolünün bu denli genişletilmesi ifade ve bilgiye erişim özgürlüğü sınırlı hale getirmektedir.
6698 Sayılı Kişisel Verilerin Korunması Kanunu	Kişisel verilerin korunması, Anayasa'nın 20. maddesiyle[102] güvence altına alınmış ve 6698 sayılı Kişisel Verilerin Korunması Kanuni (KVKK) ile detaylandırılmıştır.[103] Siber Güvenlik Kanunu'nda kişisel verilerin en fazla iki yıl süreyle saklanacağı ve sonrasında "silineceği ya da anonim hale getirileceği" ifade edilse de, bu süreçlerin denetiminden ve şeffaflığından bahsedilmemektedir. Bu durum, bireylerin verileri üzerindeki denetimini sınırlayabilecek niteliktedir.	Bireylerin şahsi verileri üzerinde kişisel kontrollerini zayıflatma riski taşıyan bu durum veri güvenliği konusunda şeffaflık ve hesap verebilirlik ilkeleriyle çelişmektedir.

Yukarıdaki tabloda görüldüğü üzere bireylerin iletişimi de içeren temel hakları anayasal güvence altına alınmıştır. Bununla birlikte yürürlüğe giren Siber Güvenlik Kanunu

97 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*, s. 28.

98 "Log" (kayıt), bilişim sistemlerinde gerçekleşen olayların, işlemlerin veya hataların kronolojik ve düzenli bir şekilde kaydedilmesini ifade eden bir terimdir. Log'lar sistemlerin izlenmesi, hataların tespiti, güvenlik ihlallerinin analizi ve performans optimizasyonu gibi kritik süreçlerde kullanılmaktadır. Kaynak: Andrew S. Tanenbaum ve Herbert Bos, *Modern Operating Systems*, Pearson, New Jersey, 2015, s. 294.

99 Siber Güvenlik Kanunu, c. 7545.

100 Türkiye Büyük Millet Meclisi, *"Basın K*anunu", Kanun No. 5187, 09 Haziran 2004, https://www.resmigazete.gov.tr/eskiler/2004/06/20040626.htm., erişim 11.06.2025.

101 Türkiye Büyük Millet Meclisi, *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"*.

102 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*.

103 Türkiye Büyük Millet Meclisi, *"Kişisel Verilerin Korunması Kanunu"*.

bireyin burada dikkat çekilen haklarını yok sayıcı birtakım ifade ve riskler içermektedir. Dolayısıyla anayasal çerçeve ihlal edilme tehlikesiyle karşı karşıya kalınmaktadır. Benzer tehlike medya içerikleri ve medyanın kamusal rolü için de geçerlidir.

4.2. *Siber Güvenlik Kanunu'nun İletişim ve Medya ile İlgili Bölümleri*

Teknolojik gelişmelerin sonucu olarak ortaya çıkan siber güvenlik meselesi multidisipliner bir alandır ve uluslararası ilişkilerden ulusal güvenliğe, siyasi uygulamalardan sosyo-kültürel yapıya, ekonomik faaliyetlerden gündelik hayat pratiklerine kadar birçok alanı birbiriyle ilişkili ve etkileşimli biçimde kapsamaktadır. Bu alanlardan en önemlilerin ikisini iletişim ve medya faaliyetleri oluşturmaktadır. İletişim ve medya faaliyetlerinin zarar verici nitelikte kullanılması güvenlik zafiyeti doğurmaktadır. Devletin ilgili kurumları bu zafiyeti ortadan kaldırmak ve adaleti tesis etmek için yasal düzenlemeler yapmaktadır. Aşağıda Siber Güvenlik Kanunu'nun[104] iletişim ve medya ile ilgili kısımları doğrudan ve dolaylı olacak şekilde sınıflandırılmıştır. Bu bağlamda Tablo 3'te yer alan sınıflandırma, Kanun'un "doğrudan" "iletişim araçları ve medya" ile tanımlanıp düzenlenen hükümlerini gösterirken, Tablo 4'teki sınıflandırma Kanun'un "veri aktarımı, altyapı kullanımı ve idari bildirim" gibi "dolaylı" iletişim boyutlarını içeren hükümlerini göstermektedir.

4.2.1. Doğrudan İletişim ve Medya ile İlgili Kısımlar

Aşağıda Siber Güvenlik Kanunu'ndaki doğrudan iletişim ve medya ile ilgili düzenlenen hükümler görülmektedir (Tablo 3).

Tablo 3. Siber Güvenlik Kanunu'ndaki Doğrudan İletişim ve Medya ile İlgili Kısımlar

Madde	İçerik	Açıklama
Madde 3(c), (i), (k)	"Bilişim sistemleri", "siber uzay" ve "varlık" tanımları	Bilgi ve iletişim teknolojileriyle sağlanan hizmetler, elektronik haberleşme ağları ve iletişim yoluyla aktarılabilen veri kavramlarıyla doğrudan iletişim kavramı ve süreci tanımlanmaktadır.
Madde 5(f)	Uluslararası bilgi alışverişi	Başkanlığın, uluslararası kuruluş ve ülkelerle "bilgi alışverişinde bulunma" yetkisi doğrudan iletişim alanıyla ilgilidir.
Madde 6(1)(c)	İletişim altyapısından yararlanma	"Elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanma, iletişim kanalında irtibat kurma" ifadesi doğrudan iletişim hakkına gönderme yapmaktadır.
Madde 12(2)	Medya yayın yasağı	Radyo, televizyon, internet, sosyal medya, gazete, dergi ve diğer tüm kitle iletişim araçlarıyla "yayınlama veya açıklama" yasağı doğrudan iletişim/medya alanına ve kitle iletişim araçlarına müdahaledir.

Tablo 3, iletişim ve medya faaliyetlerine yönelik Anayasal haklar açısından değerlendirildiğinde;

- **Madde 3(c), (i), (k):** Bu maddede "bilişim sistemleri", "siber uzay" ve "varlık" gibi temel kavramların tanımı yapılırken, iletişimin doğrudan bir bileşen olduğu kabul edilmektedir. Bu tanım, Anayasa'nın haberleşme hürriyetini düzenleyen 22. maddesiyle doğrudan ilişkilidir. Anayasa, haberleşmenin gizliliği ve engellenmemesi ilkesini esas almaktadır. Bu kapsamda iletişim teknolojilerinin tümü gizli olma ve engellenmeme ilkesinden faydalanmaktadır.

104 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*, c. 7545.

- **Madde 5(f):** Uluslararası bilgi alışverişine dair yetki verilmesi, hem ifade özgürlüğü[105] hem de bilgiye erişim hakkı[106] çerçevesinde değerlendirilebilir. Ancak bu yetkinin sınırsız veya denetimsiz kullanımı, hak ihlallerine yol açabilir.
- **Madde 6(1)(c):** "İletişim altyapısından yararlanma" doğrudan haberleşme özgürlüğüyle ilgilidir ve Anayasa'daki *"herkes haberleşme hürriyetine sahiptir"*[107] ilkesiyle uyumludur. Bu madde, bireyin elektronik kanallar üzerinden iletişim kurma hakkını tanıyarak anayasal güvence sağlamaktadır.
- **Madde 12(2):** Medya yayın yasağı getiren bu hüküm, Anayasa Madde 28'de güvence altına alınan basın özgürlüğüyle çelişebilme riskini içermektedir. Bu tür bir sınırlama, ancak Anayasa'nın 13. maddesinde belirtilen kriterlerle (kanunilik, ölçülülük, demokratik toplum gereği) sınırlanabilir. Aksi hâlde orantısız ve antidemokratik sansür anlamına gelmektedir.

Yukarıdaki maddeler (Tablo 3), doğrudan anayasal haberleşme özgürlüğü ve basın hakkıyla ilişkilidir. Anayasa'ya uygunluk, ancak sınırlamaların açık, orantılı ve yargı denetimine açık biçimde uygulanmasıyla mümkün olabilecektir.

4.2.2. Dolaylı Olarak İletişim ve Medya ile İlgili Kısımlar

Aşağıda Siber Güvenlik Kanunu'ndaki dolaylı olarak iletişim ve medya ile ilgili düzenlenen hükümler görülmektedir (Tablo 4).

Tablo 4. Siber Güvenlik Kanunu'ndaki Dolaylı Olarak İletişim ve Medya ile İlgili Kısımlar

Madde	İçerik	Açıklama
Madde 3(g)	Varlık tanımı	*"*İletişim yoluyla aktarılabilen *veri"*yi kapsasa da, burada iletişim altyapısından ziyade varlığının kapsamı tanımlanmaktadır. Kavramın soyut uzamına müdahale edilmektedir.
Madde 6(1)(b)	Veri ve log aktarımı	"Ürünler tarafından üretilen veya toplanan veri ve log kayıtlarının Başkanlık sistemlerine aktarılması" dolaylı iletişim (veri işleme) faaliyetidir. Denetim mekanizmasının yetkisi artırılmıştır.
Madde 6(1)(c)	Uzaktan müdahale desteği	Siber olay müdahale desteğinin "yerinde veya uzaktan" sağlanması, teknik iletişim kanalları üzerinden koordinasyon anlamına gelir. Denetim mekanizmasının yetkisi artırılmıştır.
Madde 7(1)(a-b)	Bildirim ve katkı yükümlülüğü	Kurum ve kuruluşların "talep edilen veri, bilgi, belge ve katkıyı zamanında iletme" sorumluluğu, idari iletişim süreçlerine işaret eder. Denetim mekanizmasının yetkisi artırılmıştır.
Madde 8(4)	Denetimde elektronik inceleme	Denetime konu doküman, sistem ve iletişim altyapısının incelenmesi yetkisi, esasen denetim amaçlı dolaylı iletişim (erişim) faaliyetidir. Denetim mekanizmasının yetkisi artırılmıştır.

Tablo 4'teki maddeler iletişimle dolaylı olarak bağlantılı olmakla birlikte anayasal açıdan dikkatle alınması gereken durumlar içermektedir:

- **Madde 3(g):** "Varlık" tanımı ile veri kavramı genişletilirken, bireylerin iletişim verilerinin de bu kapsama alınması mümkün hâle gelmektedir. Bu durum, kişisel verilerin korunması hakkı ve özel hayatın gizliliğiyle (Anayasa Madde 20) ilgilidir.

105 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*, Md. 26.
106 Age, Md. 74.
107 Age, Md. 22.

- **Madde 6(1)(b):** Veri ve log aktarımı, bireylerin dijital faaliyetlerine dair izleme ve kayıt tutma anlamına gelmektedir. Bu uygulama, Anayasa Madde 22'deki haberleşmenin gizliliği ilkesini ilgilidir. Log'ların izinsiz veya sürekli toplanması, ölçülülük ve orantılılık ilkesini ihlal edebilecek riski taşımaktadır.
- **Madde 6(1)(c):** Uzaktan müdahale desteği, haberleşme sistemlerine dışarıdan erişim anlamına gelmektedir. Bu durum da Anayasa Madde 22'nin koruduğu haberleşmenin gizliliğine müdahale niteliği taşımaktadır. Burada meşruiyeti sağlamak için uygulamanın yalnızca yasal ve denetimli çerçevede yapılması koşulu yerine getirilmelidir.
- **Madde 7(1)(a-b):** Bildirim ve katkı yükümlülüğü, kurumların belge sunma yükümlülüğünü düzenlerken idari süreçlerde iletişimi doğrudan etkilemektedir. Bu tür yükümlülüklerin Anayasa'nın "adil yargılanma" ve "özel hayat" hükümleriyle (Madde 36 ve Madde 20) dengelenmesi gerektiği görülmektedir.
- **Madde 8(4):** Elektronik denetim yetkisi, iletişim altyapısına müdahale imkânı sunmaktadır. Bu durum, haberleşmenin ve verilerin denetlenmesi anlamına geldiğinden, ancak mahkeme kararıyla ve sınırlı şekilde yürütüldüğünde Anayasa'ya uygun olabilecektir.

Yukarıdaki maddeler (Tablo 4) dolaylı da olsa iletişim özgürlüğü ve özel hayatın gizliliği gibi temel haklara müdahale niteliği taşımaktadır. Müdahalenin Anayasal ilkelere uygunluğu güç kullanımında ölçülülük, yasal dayanaklılık ve yargı denetimine açıklık (şeffaf) şeklinde yapılmasıyla mümkündür.

Her iki tabloya göre Siber Güvenlik Kanunu'nda yer alan düzenlemeler, anayasal haberleşme özgürlüğü (Madde 22), ifade ve basın özgürlüğü (Madde 26-28), özel hayatın gizliliği (Madde 20) ve bilgiye erişim hakkı (Madde 74) ile yakından ilişkilidir. Bu düzenlemelerin hukuk devleti ilkesine uygun olarak yürütülmesi; ölçülülük, kanunilik ve demokratik toplum ilkeleri doğrultusunda yorumlanması gerekmektedir. Özellikle iletişim ve medya üzerindeki doğrudan ve dolaylı düzenlemelerin yargı denetimine açık olması, temel hakların korunması açısından zorunludur. Tüm bunlar ilgili yasal düzenlemenin yeterli şeffaflığı sağlamadığı ve olumsuz sonuçlanabilecek uygulamalara yol açabileceğini göstermektedir.

4.3. İletişim Süreçleri ve Medya Faaliyetlerine Yönelik Uluslararası Sözleşmeler

Türkiye'de iletişim ve medya faaliyetleri hukuki açıdan uluslararası sözleşmeler, Türkiye Cumhuriyeti Anayasası ve iletişim ile güvenlik alanındaki temel yasa ve mevzuatlar ile düzenlemektedir. Uluslararası düzeyde İfade Özgürlüğü ve İletişim Hürriyeti Hakkı, Uluslararası Medeni ve Siyasi Haklar Sözleşmesi (ICCPR) ve Avrupa İnsan Hakları Sözleşmesi (ECHR) ile güvence altına alınmıştır. ICCPR, ifade ve bilgi alma-verme özgürlüğünü korumaktadır ancak diğer yandan aynı metinler, "ulusal güvenlik" ve "kamu düzeni" gerekçesiyle iktidara "meşru, orantılı ve kanunda öngörülmüş" düzeyde güç kullanma ya da bazı özgürlükleri "kısıtlama"[108] veya "sınırlama" hakkı [109] vermektedir.

108 United Nations, "International Covenant on Civil and Political Rights, ICCPR", United Nations Treaty Series, 1967, https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf?utm, erişim 18.05.2025; The Council of Europe, "European Convention on Human Rights", The Council of Europe Publishing, Rome, 4.XI.1950, 1950, https://www.eods.eu/library/CoE_European%20Convention%20for%20the%20Protection%20of%20Human%20Rights%20and%20Fundamental%20Freedoms_1950_EN.pdf?utm, erişim 12.06.2025.

109 United Nations, *"Article 19: Freedoms of Opinion and Expression"*, United Nations Human Rights Committee, July 2011, https://www.refworld.org/legal/general/hrc/2011/en/83764, erişim 12.06.2025.

Ayrıca ECHR, devletlerin "radyo, televizyon veya sinema kuruluşlarının lisanslanması" gibi teknik sınırlamalarını da meşru kabul etmektedir.[110] Yukarıdaki sınırlama veya kısıtlamalar demokratik bir toplumda "gerekli" olmakla birlikte zorunlu kıstas "ölçülü" ve "şeffaf" olmasıdır.[111]

Türkiye'de ise ifade ve haberleşme özgürlüğünün sınırları temel Anayasal haklar[112] İnternet Ortamında Yapılan Yayınlar[113], Elektronik Haberleşme[114] Kişisel Verilerin Korunması[115] ve en son 2025'te yürürlüğe giren Siber Güvenlik Kanunu[116] ile çerçevelenmiştir ve bu çerçeve iktidara güvenlik gerekçelerini öne sürerek iletişim süreçlerine müdahale yetkisi tanımaktadır. Bu bağlamda İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun içerik ve erişim sağlayıcıları alanlarını düzenleyerek, yetkili kurumlara "kamu güvenliği" ve "suç önleme" gerekçesiyle içerik kaldırma ve erişim engelleme yetkisi tanımaktadır. Yargı kararı veya Bilişim Teknolojileri Kurumu (BTK) kararıyla anlık müdahaleye imkân tanınmaktadır.[117] Elektronik Haberleşme Kanunu, telekomünikasyon işletmecilerine haberleşme verilerini "gizli" tutma yükümlülüğü getirirken, "milli güvenlik", "ulusal savunma", "suç soruşturması", "kamu düzeni" ve "kamu güvenliği" gibi gizliliği ortadan kaldıran istisnalara yer vermektedir.[118] Siber Güvenlik Kanunu ise yetkili mercilerin iletişim altyapıları üzerindeki denetimini genişleterek, "siber tehdit istihbaratı" toplama ve yayma, "Log" kayıtlarına müdahale, veri merkezlerinde arama ve kopya alma gibi olağanüstü yetkiler tanımaktadır.[119] Türk Ceza Kanunu'na göre haberleşmenin gizliliğini ihlal edenlere ve iletişim verilerine izinsiz erişim sağlayanlara, suçun niteliğine göre farklı oranlarda hapis ve/veya para cezası öngörülmektedir.[120]

Yukarıda değinilen kanuni düzenlemelerin ihlali "siber suç" kapsamına girmektedir. Siber suç, literatür bölümünde de değinildiği üzere, bilişim teknolojileri aracılığıyla hem bireysel ve toplamsal açıdan zarar verici, hem de ulusal güvenliği ve kamusal düzeni zedeleyici nitelikler taşımaktadır. Bu bağlamda iletişim ve medya faaliyetleri ile güvenlik arasındaki denge, hem uluslararası hem de ulusal hukukta Anayasa, kanun ve sözleşmelerle düzenlenmiştir. Yapılan düzenlemeler sorunu çözme noktasında önemli katkılar sunmaktadır fakat aynı zamanda hak ve özgürlükleri kısıtlayıcı nitelikler de taşımaktadır. Bir başka ifadeyle, birey ve toplumun sağlıklı bir ortamda yaşaması için oluşturulan kanun ve uygulamaların tersi yönünde de etkileri ortaya çıkarak kamusal alana zarar verme riskini gündeme getirmektedir. Literatürde bu durumu dikkat çeken birçok yaklaşım bulunmaktadır. Aşağıda bu yaklaşımlardan Habermas'ın Kamusal Alan kavramsallaştırmasından yola çıkılarak Kanun'un ortaya çıkardığı olumsuz durum ve risk potansiyeli analiz edilmiştir.

110 The Council of Europe, *"European Convention on Human Rights"*.
111 The Council of Europe, *"Guide on Article 10 of the European Convention on Human Rights", The Council of Europe* Publishing, Strasbourg, 2021. https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/11/Guide_Art_10_ENG.pdf, erişim 12.06.2025.
112 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*.
113 Türkiye Büyük Millet Meclisi, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, c. 5651.
114 Türkiye Büyük Millet Meclisi, *"Elektronik Haberleşme Kanunu"*.
115 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu*.
116 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.
117 Ebru Çetin, "Kitle İletişim Aracı Olarak İnternet ve Hukuk İlişkisi: Türkiye Örneği", *Sosyoloji Dergisi,* 33, 2016, s. 5.
118 Şehriban İpek Aşıkoğlu, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-", *Kişisel Verileri Koruma Dergisi*, 1:2, 2019, ss. 55-56.; Reyhan Karcı, "Ulusal Hukukta Kişisel Verilerin Korunması Hakkına İlişkin İstisnai Haller", Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy (Ed.), *Kişisel Verilerin Korunmasına Uzman Bakışı*, KVKK Yayınları, Ankara, 2023, s. 265.
119 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.
120 Pınar Kartal ve Gülfem Işıklar Alptekin, "Türk Ceza Hukukunda Bilişim Sistemine Girme Suçuna İlişkin Değerlendirmeler", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 29:1, 2023, s. 18.

5. Habermas'ın Kamusal Alan Yaklaşımı ve Siber Güvenlik Kanunu Açısından Analizi

Habermas'ın Kamusal Alan kavramı, demokratik siyasetin rasyonel-kritik tartışma zeminini, bu zeminin tarihsel koşullarını ve modernleşme ile birlikte kamusal alanın dönüşümünü açıklamaktadır. Bu yönüyle, iletişim ve medya düzenlemelerinin anayasal etkilerini değerlendirmek için güçlü bir kuramsal araç sunmaktadır.[121] Dolayısıyla siber güvenlik düzenlemesinin medya/iletişim üzerindeki etkisini değerlendirirken, metnin kamusal tartışmayı nasıl dönüştürdüğünü, hangi aktörlere yetki verdiğini ve kamusal alanın niteliğini nasıl etkilediğini Habermasçı kıstaslarla sorgulamak uygun olacaktır. Aşağıdaki tabloda (Tablo 5), Habermasçı yaklaşımın ölçütlerinin temel çerçevesi yer almaktadır:

Tablo 5. Habermas'ın Kamusal Alan Analizi

Analitik Çerçeve	Habermasçı Ölçütler
Erişilebilirlik ve Kapsayıcılık	Kamusal alanın tartışmaya açık, eşit erişime imkân veren bir alan olması gerekir.[122]
Rasyonel-Kritik Tartışma	Kamuoyunun neden temelli, gerekçeye dayanan tartışmalara elverişli olması; çıkar-odaklı propagandaya dönüşmemesi gerekir.[123]
Özerk Medya-Aracı Rolü	Medyanın kamusal denetim ve bilgi sağlama işlevini, devletin tek yanlı yönlendirmesinden korunmuş biçimde yerine getirebilmesi gerekir.[124]
Kamusallıkla Bürokratik-Kamusal İktidarın Ayrımı	Devlet/idare ile kamusal tartışma alanı arasındaki sınırları belli olmalıdır. Devletin bünyesindeki güçlerin de kamusal tartışmayı ("refeodalizasyon" riski) bağlamında bu sınırlar içinde tutması gerekir.[125]

i. Kamusal Alanın Erişilebilirliği ve Kapsayıcılık Ölçütü Analizi

Habermas'a göre kamusal alanın demokratik işlevi, farklı toplumsal aktörlerin rasyonel-kritik tartışmaya erişebilmesiyle doğru orantılıdır.[126] Siber Güvenlik Kanun'un "her türlü medya aracıyla açıklama yasağı" (m. 12–13) gibi geniş kapsamlı sınırlamalarının kamuoyunun erişim ve katılım kanallarını daraltma potansiyeli taşıması[127] kamusal alanın erişebilirliği ve kapsayıcılık ölçütüyle çakışmaktadır. Eğer devletin kurumları bilgi ve tartışma alanlarını tek taraflı biçimde kapatma yetkisine sahip ise, kamusal tartışmanın kapsayıcılığı ve dolayısıyla demokratik meşruiyeti zarar görecektir.

ii. Rasyonel-Kritik Tartışmanın Zedelenmesi Ölçütü Analizi

Habermas'ın ideal kamusal alanı, argümanların en iyi gerekçenin lehine geliştiği; manipülasyonun, pazarlama ve propaganda mekanizmalarının hâkim olmadığı bir alandır.[128] Siber Güvenlik Kanunu'nun geniş yetki tanıyan düzenlemelerinin (idarenin geniş takdir yetkisi ve gizlilik istisnaları gibi[129]) kamunun haber alma, eleştirel kamuoyu oluşturma, denetimi zayıflattığı için kamusal tartışmanın niteliğiyle çakışmaktadır. Başka bir ifadeyle, devletin bilginin dolaşımını kısıtlamaya yönelik mekanizmalarının eleştirel tartışmayı değil, yönlendirilmiş veya susturulmuş bir kamuoyu üretme riskini artırması kamusal-aklın zayıflaması anlamına gelmektedir.

121 Jurgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Çev. Thomas Burger), MIT Press, Cambridge, 1989, s. 40.
122 Age, s. 36.
123 Age, ss. 89-109.
124 Habermas, *The Structural Transformation of the Public Sphere*: An Inqu*iry into a Category of Bourgeois Society*, s. 165.
125 Age, s. 232.
126 Age, s. 36-40.
127 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.
128 Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, s. 89-103.
129 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.

iii. Medya Kuruluşlarının Özerkliği ve Kamu-Siyaset Ayrımı Ölçütü Analizi

Habermas'a göre ideal kamusal alanda faydaya yönelik toplumsal düşüncenin etkin olması gerekmektedir. Oysa kitlesel medya, etki alanını derinleştiren dönüşümüyle birlikte kamu otoritesi ve pazar güçlerini kamusal alan üzerinde etkili hâle getirmektedir. Bu da kamusal tartışmaları ticarileştirme ve/veya devletleştirme sonucunu doğurmaktadır.[130] Siber Güvenlik Kanunu'nda tarif edilen yetki genişlemeleri, Habermasçı risk profiliyle örtüşmekte ve dolayısıyla devletin iletişim üzerinde geniş idari müdahale hakları medyanın özerk kamusal tartışma işlevini zayıflatabilme riskini ortaya çıkarmaktadır.

iv. Yönetimsel Güç ve "Refeodalizasyon" Riski

Habermas'ın kamusal alanla ilgili tarihsel analizinde, bürokrasinin ve pazarın kamusal alanı içselleştirip onun işlevini bozduğu "refeodalizasyon" uyarısı önemli yer tutmaktadır.[131] Siber Güvenlik Kanunu'nun vurguladığı yürütme-odaklı yetki tahsisinin[132] şeffaflık ve yargısal denetim mekanizmalarını zayıflatmaya yönelik olması, kamusal alanda güçlü aktörlerin (devlet bürokrasisi ve sermayenin) kamusal gündemi belirleme potansiyelini güçlendirmektedir. Sonuç olarak, yeni bir feodal etki oluşturulduğu için kamusal alanın "entelektüel özerkliği" zedelenmektedir.

Yukarıdaki ölçütler bağlamında, karar süreçlerinin kamuya açıklanabilir derecede şeffaf bir yapı sağlanmasının yanında yargısal denetimin müdahale yetkileri açık ve yargısal denetime tabi olmalıdır. Kanuni düzenlemeler kamusal tartışma alanını kapatmamalıdır. Bağımsız denetim kurumları ve sivil toplum örgütlerinin **güçlendirilerek kam**usal alanın işlevinin korunması sağlanmalıdır.

5.1. Habermas'ın Kamusal Alan Perspektifi Bağlamında Siber Güvenlik Kanunu'nun İletişim Süreçleri ve Medya Faaliyetlerinin Değerlendirmesi

Siber güvenlik ve hukuk arasındaki ilişki, Habermas'ın kamusal alan teorisi açısından değerlendirildiğinde, modern iletişim sistemlerinin yapısal dönüşümünün dijital ortamda yeni bir evreye ulaştığı görülmektedir. Habermas'a göre kamusal alan, yurttaşların serbestçe bir araya gelerek kamusal meseleler üzerine tartışabildikleri, devlet ile toplum arasındaki aracı alanı ifade etmektedir.[133] Dijitalleşen dünyada bu alan, yalnızca fiziksel mekânlarla sınırlı olmayıp, çevrim içi platformlar ve sosyal medya aracılığıyla genişlemiştir. Ancak siber güvenlik düzenlemeleri ve özellikle de Türkiye'de 2025 yılında yürürlüğe giren Siber Güvenlik Kanunu, bu alanın sınırlarını yeniden çizmektedir.

Habermas'ın İletişimsel Eylem Kuramı, toplumsal uzlaşıya ulaşmanın temel yolunun rasyonel, şeffaf ve eşitlikçi iletişim süreçleri olduğunu vurgulamaktadır.[134] Bu perspektiften bakıldığında, siber güvenlik politikaları yalnızca teknik koruma mekanizmaları değil, aynı zamanda iletişimin yapısını ve yönünü belirleyen güç ilişkilerinin de ürünüdür. Hukuki düzenlemeler, kamusal alanın özgür tartışma kapasitesini güçlendirebilme potansiyeline sahiptir ancak hukuk yoluyla aşırı denetim, iletişimsel rasyonaliteyi zayıflatma riski taşımaktadır.

130 Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, s. 196-232.

131 Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, s. 232.

132 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.

133 Habermas, *The Structural Transformation of the Public Sphere: An inquiry into a Category of Bourgeois Society*, s. 27.

134 Habermas, *The Theory of Communicative Action, Volume One: Reason and the Rationalization of Society*.

Siber güvenlik ve hukuk etkileşimi, çok hukuklu bir yapıya evrilirken, bu normatif çoğulluk iletişimsel eylem süreçlerinde yeni sorunlar doğurmaktadır. Örneğin, farklı kural koyucuların (devlet, devletin yetkilendirdiği kurumlar, uluslararası örgütler, teknoloji şirketleri vb.) siber alanda eş zamanlı etkili olması, Habermas'ın yaşam dünyasının sömürgeleştirilmesi kavramıyla açıklanabilecek bir durumu ortaya çıkarmaktadır.[135] Devletin güvenlik gerekçesiyle dijital iletişim alanını düzenlemesi, bireylerin kamusal tartışmalara katılımını sınırlayabilme ve iletişim alanını piyasa/sermaye ya da bürokrasi mantığıyla şekillendirme olasılığını artırmaktadır.

Bu bağlamda, 2025 tarihli Siber Güvenlik Kanunu'nun anayasal haklar, iletişim sosyolojisi, medya çalışmaları ve siyasal iletişim açısından iki yönlü bir etkisi olduğu görülmektedir. Bir yandan, siber tehditlere karşı kamusal güvenliği artırarak kamusal alanın güvenli işleyişini sağlamayı hedeflerken, diğer yandan, iletişim akışını düzenleme ve denetleme yetkisi, kamusal tartışma özgürlüğü üzerinde sınırlayıcı etki oluşturmaktadır. Habermas'ın demokratik meşruiyet vurgusu dikkate alındığında,[136] bu tür düzenlemelerin meşruluğu, ancak kapsayıcı, şeffaf ve yurttaşların katılımına açık karar alma süreçleriyle sağlanabilecektir.

Sonuç olarak, siber güvenlik ile hukuk arasındaki ilişki, Habermas'ın Kamusal Alan ve İletişimsel Eylem Teorisi çerçevesinde değerlendirildiğinde hem güvenlik hem de özgürlük boyutlarının dengelenmesini gerektiren dinamik bir alan olarak karşımıza çıkmaktadır. Türkiye'de yürürlüğe giren Siber Güvenlik Kanunu, dijital kamusal alanın sınırlarını ve işleyişini doğrudan etkileyen bir düzenleme olarak, kurumların şeffaf faaliyetleri ve demokratik iletişim kültürünün korunması açısından dikkatle izlenmelidir.

Sonuç ve Öneriler

Dijitalleşmenin yaygınlaşmasıyla birlikte siber güvenlik konusu hem bireysel hakların korunması, hem ulusal güvenlik, hem de uluslararası ilişkiler ve uluslararası güvenlik açısından merkezi bir politika alanı haline gelmiştir. Türkiye'de 19 Mart 2025'te yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, teknolojik tehditlere karşı hukuki boşlukları kapatmayı ve kapsamlı bir savunma mekanizması kurmayı amaçlamaktadır. Ancak kanunun iletişim ve yeni medya faaliyetleri üzerindeki doğrudan ve dolaylı etkileri, özgürlük–güvenlik dengesi açısından ciddi tartışmalara açıktır. Örneğin, son dönem hukuk felsefesinin önemli isimlerinden Rawls'un adalet prensiplerine göre güvenlik politikalarının temel hakların korunması adaletin öncelikli koşuludur.[137] Oysa Kanun'un genel çerçevesi bu koşulu görmezden gelinmeye açık hâle getirmektedir. Gözetim kuramlarının tümünde olduğu gibi[138], Solove'un mahremiyet analizlerine göre Kanun'un yetki kapsamı toplanan verinin kullanım biçimlerinin çeşitli zararlar doğurabileceğini göstermektedir.[139]

Floridi'nin "bilgi etiği" kuramına göre geniş log toplama, uzun süreli saklama, merkezi veri aktarımı ve medya kısıtlamaları infosferin bütünlüğünü ve bireylerin bilgi özerkliğini zedeleyerek bilgi varlıklarına etik zarar riski doğurduğundan, bu müdahalelerin

135 Jurgen Habermas, *The Theory of Communicative Action, Volume Two: Lifeworld and System: A Critique of Functionalist Reason* (Çev. Thomas McCarty), Beacon Press, Boston, 1987, s. 232.

136 Jurgen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (Çev. William Rehg), MIT Press, Cambridge, 1996, s. 307.

137 Rawls, *Bir Adalet Teorisi*.

138 Zygmunt Bauman, *Akışkan Gözetim* (Çev. Elçin Yılmaz), Ayrıntı Yayınları, İstanbul, 2016.; Castells, *Ağ Toplumunun Yükselişi*; Deleuze & Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*; Foucault, *Hapishanenin Doğuşu*.

139 Solove, *Understanding Privacy*.

"zarar vermeme", ölçülülük, şeffaflık, denetlenebilirlik ve bilgi yöneticiliği (*stewardship*) ilkeleri[140] bağlamında Kanun'un açık şekilde sınırlandırılması gerektiğini göstermektedir. Baudrillard'ın teknolojinin/dijitalleşmenin geldiği aşamayı tartıştığı "simülasyon/simülakr" kuramında sanal olanın gerçeğin yerine geçtiğine yönelik "hipergeçeklik" kavramsallaştırmasına[141] referansla, siber uzay üzerindeki devlet müdahalelerinin gerçek dünyadaki iletişim ve toplumsal ilişkiler üzerinde derin etkileri olması, siber uzayda olan her şeyin gündelik hayatın her anını ve özellikle iletişim süreçleri ve medya faaliyetleri üzerinde de büyük bir etkiye sahip olduğunu göstermektedir. Dolayısıyla buradaki adımların daha dikkatli atılması kamusal fayda için bir zorunluluktur. Buradan da anlaşılacağı üzere, Kanun'un yetkilendirme ve icraat boyutları medya faaliyetleri de dâhil tüm iletişim süreçlerinde olduğu kadar kişisel bilgi ve mahremiyet haklarına yönelik ihmal veya kasıtlı/keyfi uygulamaları zemin hazırlama potansiyeline sahiptir. Kuramsal örnekler çoğaltılabilir çünkü Kanun literatürün (teknoloji, güvenlik, kültür, siyaset özgürlük, adalet, kişisel haklar vb.) tartıştığı birçok kuramsal yaklaşımla değerlendirilebilir niteliktedir. Kapsamı daraltan bu çalışma, Kanun'un iletişim süreçleri ve yeni medya üzerindeki etkilerini anayasal haklar perspektifiyle Habermas'ın Kamusal Alan kavramı çerçevesinde uluslararası sözleşmelere de değinerek analiz etmiştir.

Kanun'un 12. maddesi radyo, televizyon, internet ve sosyal medya dâhil tüm kitle iletişim araçlarıyla yapılan yayınlara yönelik yasaklar getirmekte; m. 12(2) gibi hükümler medyaya geniş kapsamlı kısıtlamalar öngörmektedir. Bu düzenlemeler, Türkiye Cumhuriyeti Anayasası'nda güvence altına alınmış olan basın (m. 28) ve ifade özgürlüğü (m. 26) ile Avrupa İnsan Hakları Sözleşmesi (AİHS/ECHR) Madde 10'un "demokratik toplum gerekliliği", "gerekli ve orantılı" kısıtlama kriterleri açısından sorunlu bir zemin oluşturmaktadır. Mevcut hâliyle bu kısıtlamaların ölçülülük, açıklık ve yargısal denetime yeterince tâbi olmadığı ve bunun sansür riskinin yanında keyfî uygulamalara zemin hazırladığı anlaşılmaktadır.

Madde 6(1)(c) uyarınca yetkililere tanınan iletişim altyapısına uzaktan müdahale yetkisi, haberleşmenin gizliliği ve Anayasa'nın haberleşme hürriyeti (m. 22) ile açıkça çatışma potansiyeli taşımaktadır. Bu tür doğrudan müdahaleler, kamusal tartışma ortamını zayıflatmakta ve Habermas'ın iletişimsel eylem perspektifinden bakıldığında kamusal diyaloğun özerkliği zarar görebilmektedir.

Madde 7(1)(a–b) ile kurumlara yüklenen "veri ve log aktarımı" yükümlülüğü; log kayıtlarının iki yıl saklanması ve anonimleştirme süreçlerinin denetimsizliği, kişisel verilerin korunması ilkeleri ve özel hayatın gizliliği (Anayasa m. 20; KVKK) ile uyumlu görünmemektedir. Madde 6(1)(b) kapsamında Başkanlığa aktarılan log kayıtları iletişimin gözetlenmesi anlamına gelmektedir. Solove'un çok boyutlu mahremiyet analizine göre bu tür uygulamalar bireylerin bilgi özerkliğini zayıflatmaktadır. Anonimleştirme uygulamalarının şeffaf olmaması ve denetim mekanizmalarının belirsizliği, veri suiistimaline ve sosyal mühendislik yoluyla kötüye kullanıma zemin hazırlayabilme riskini taşımaktadır.

Madde 3(c), (i) ve (k) ile tanımlanan "bilişim sistemleri" ve "siber uzay" gibi kavramlar, iletişim özgürlüğünü doğrudan etkileyen teknik düzenlemeleri içermektedir. Ancak bu tanımların ve düzenlemelerin Anayasa'nın öngördüğü hukuki güvencelerle (yasallık ilkesi) birlikte demokratik toplum bağlamında ölçülülük ve gereklilik kriterlerini sağlayıp sağlamadığı tartışmalıdır. Teorik olarak uygulama süreçlerine kanunilik yeterli olsa bile demokratik denetim kriterlerinin gözetilmememe sorunu ortaya çıkmaktadır.

140 Floridi, *"Information Ethics: On the Philosophical Foundation of Computer Ethics"*.
141 Jean Baudrillard, *Simülasyon ve Simülakr* (Çev. Oğuz Adanır), Doğu Batı Yayınları, Ankara, 2011, s. 13.

BM, AB ve NATO gibi kuruluşların siber güvenlik politikaları genellikle şeffaflık ve insan hakları odaklı standartlar içerirken, Türkiye'deki düzenlemelerde "ulusal güvenlik" vurgusunun geniş tanımlanması bu standartlardan sapma riski taşımaktadır. Özellikle Madde 5(f) ile Siber Güvenlik Başkanlığı'na verilen "uluslararası bilgi alışverişi" yetkisinin kapsam ve denetiminin belirsiz olması uluslararası normlarla uyum kaygısını artırmaktadır. Yerel mevzuata uluslararası normların yeterince entegre edilmemesi, uzun vadede iş birliğini zayıflatabilme ve politikaların meşruiyetini azaltma riski taşımaktadır.

Madde 8(4) ile yetkililere tanınan "elektronik inceleme" yetkisi ve sistemlere ilişkin denetim kapasitesinin genişletilmesi, iletişim altyapısında kalıcı gözetim mekanizmalarının kurulmasına yol açabilecek niteliktedir. Schlink'in devlet koruma sorumluluğu ile bireysel özgürlükler arasındaki gerilim vurgusu burada görünür hâle gelmektedir. Kanun ile doğrudan yasaklamanın ötesinde, gözetim ve veri işleme süreçleri üzerinden yürüyen dolaylı müdahaleler devletin otoriterliği bağlamında daha yaygın ve kalıcı etkiler doğurabilecek potansiyele sahiptir.

Yukarıdaki özet, Kanun'un genel çerçevesinin Habermas'ın ideal kamusal alan kavramındaki toplumsal faydaya yönelik açıklamalarıyla tezatlık göstermektedir. Habermas'ın Kamusal Alan Teorisi, kamusal tartışmanın serbestliği ve toplumsal uzlaşının iletişimsel yollarla sağlanmasının önemini ortaya koymaktadır. Bu bağlamda değerlendirildiğinde, Kanun'un mevcut düzenlemelerinin hem kamusal alanın işlevselliğini zayıflatma hem de adalet ve mahremiyet standartlarıyla çelişme riski taşıdığı sonucuna ulaşılmaktadır. Yine bu çerçeveye göre Siber Güvenlik Kanunu'nun getirdiği geniş kapsamlı kısıtlamalar ve denetimsizlik riski, kamusal tartışmanın sağlıklı işlemesi için gerekli olan iletişimsel koşulları zedelemektedir. Habermas'a göre kamusal alan, farklı toplumsal aktörlerin eşit koşullarda rasyonel-eleştirel tartışmaya katıldığı ve kamuoyunun özgürce oluştuğu bir mekân ve/veya ortamdır. Bu mekân ve/veya ortamın işlerliği, sansürsüz ifade, erişim serbestliği ve konuşma alanının korunmasına dayanmaktadır. Kanun'un medya üzerindeki yayın yasakları, altyapıya müdahale yetkileri ve geniş veri toplama uygulamaları, eşitlikçi ve açıklığa dayalı iletişim koşullarını bozarak kamusal aklın oluşumunu engelleyebilme potansiyelini taşımaktadır. Bu şekilde oluşan kamusal alanda ise toplumun kendini yöneten bir kamuoyuna dönüşme kapasitesinin zayıflama ihtimali yüksektir.

Bu nedenle Habermasçı perspektif, politika önerilerini normatif bir zemine oturtmak için yol göstericidir. Kamusal alanın korunması, sadece ifade özgürlüğünün teknik garantileriyle değil, aynı zamanda şeffaflık, bağımsız denetim ve yargısal denetim mekanizmalarının tesis edilmesiyle mümkündür. İleri teknoloji ve güvenlik gerekçeleriyle yapılan düzenlemeler, kamusal tartışma alanının asgari koşullarını koruyacak şekilde yeniden biçimlendirilmelidir. Aksi takdirde güvenlik politikaları, kamusal rasyonaliteyi ve demokratik meşruiyeti zayıflatma riski taşıyacaktır. Habermas'ın vurguladığı iletişimsel eylem ve kamusal rasyonalite ilkeleri, Kanun'un uygulanmasında ölçülülük, hesap verebilirlik ve katılımcılığı güçlendirecek reformların temel normatif dayanağını oluşturmaktadır.

Kanun'un iletişim ve medya üzerindeki olumsuz etkilerini azaltmak ve anayasal/uluslararası normlarla uyumu sağlamak için şu tedbirler önerilmektedir:

i. Ölçülülük ve Yargısal Denetim: Kısıtlayıcı hükümlerin Anayasa m. 13'te belirtilen "demokratik toplum gerekliliği" çerçevesinde yeniden tanımlanarak tüm istisnai tedbirler bağımsız yargı denetimine tabi kılınmalıdır.

ii. Şeffaf Veri Yönetimi ve Bağımsız Denetim: Log ve kişisel veri toplama/saklama süreçleri için şeffaf veri yönetimi, açık kurallar, denetlenebilir yapılar ve bağımsız denetim mekanizmaları oluşturulmalıdır.

iii. Uluslararası Uyum: BM, AB ve NATO gibi uluslararası kuruşların standartlarıyla uyumlu mevzuat uyarlamaları yapılarak uluslararası normlarla entegrasyon sağlanmalıdır.

iv. Siber Okuryazarlık ve Adalet Bilinci: Toplum, medya çalışanları ve sivil toplum dijital haklar, veri güvenliği ve yeni medya okuryazarlığı konularında eğitilerek hak ve sorumluluk bilinci güçlendirilmelidir.

v. Teknoloji-Politika Entegrasyonu: Siyaset kurumu ve bürokratik yapının hızla şekilde sektörle birlikte hareket etmesi sağlanmalı ve yapay zekâ, blokzincir gibi ileri teknolojilerin mevzuata entegrasyonu konusunda disiplinlerarası düzenlemeler geliştirilmelidir.

vi. Alanyazın Çalışmaları: Gelecek araştırmalar Kanun'un uygulamadaki yansımalarını izlemeye odaklanarak medya mensupları, sivil toplum ve hukukçuların deneyimleri temel alınarak niteliksel çalışmalar yoğunlaştırılmalıdır. Ayrıca ileri teknolojilerin (yapay zekâ, blokzincir vb.) iletişim süreçleri, ifade özgürlüğü ve mahremiyet ve medya faaliyetleri üzerindeki etkileri bakımından disiplinlerarası nitelikli araştırmalar yapılmalıdır.

Sonuç olarak, 7545 sayılı Siber Güvenlik Kanunu teknolojik tehditlere karşı önemli engelleyici mekanizmalar getirse de uygulama biçimi ve denetim eksiklikleri nedeniyle ifade ve iletişim özgürlükleri ile özel hayatın gizliliği açısından ciddi riskler barındırmaktadır. Kanun'un demokratik meşruiyeti ve uzun vadeli etkinliği, şeffaflık, ölçülülük, yargısal denetim ve uluslararası standartlarla uyum yoluyla güvence altına alınmalıdır. Bu çalışma, siber güvenlik ile iletişim özgürlüğü arasındaki adalete dayalı, katılımcı dengenin nasıl kurulabileceğine yönelik hem akademik hem de politika yapıcı tartışmalara katkı sunmayı amaçlamıştır.

Çıkar Çatışması

Bu çalışmada çıkar çatışması teşkil edebilecek durum ve/veya ilişki bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Bu çalışma oluşturulurken, araştırma konusuyla ilgili Türkçe dışındaki literatürün daha iyi anlaşılabilmesi amacıyla çeviri desteği almak ve metnin bazı bölümlerinde daha akıcı bir dil oluşturmak için yapay zekâdan yararlanılmıştır.

KAYNAKÇA

Basılı Kaynaklar

AKÇAKANAT Özen ÖZDEMİR Ozan ve MAZAK Mehmet (2021). "İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi", *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi*, 5:2, 246-270.

AKSOĞAN Mustafa BAYER Harun GÜLADA Mehmet Ozan ve ÇELİK Enes (2018). "İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği", *Kesit Akademi Dergisi,* 13, 271-288.

AKYEŞİLMEN Nezir (2018). *Disiplinlerarası Bir Yaklaşımla: Siber Politika & Siber Güvenlik*, Orion Kitabevi, Ankara.

ALTINTOP Mevlüt (2021). *Zygmunt Bauman Sosyolojisinde İletişim Olgusu*, Kitapyurdu Doğrudan Yayıncılık, İstanbul.

ANDERSON Ross (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*, (3. Baskı), Wiley, New York.

AŞIKOĞLU Şehriban İpek (2019). "Veri Sorumlularının Aydınlatma Yükümlülüğü-Avrupa Birliği ve Türk Hukukunda-", *Kişisel Verileri Koruma Dergisi*, 1:2, 41-65.

ATA Zeynep (2024). "Sosyal Medyada Suç Korkusunun Oluşması ve Yayılması: X Örneği", *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 37, 382-398.

AVŞAR Zakir ve ÖNGÖREN Gürsel (2010). *Bilişim Hukuku*, Türkiye Bankalar Birliği, İstanbul.

BAUDRILLARD Jean (2011). *Simülasyon ve Simülakr* (Çev. Oğuz Adanır), Doğu Batı Yayınları, Ankara.

BAUMAN Zygmunt (2016). *Akışkan Gözetim* (Çev. Elçin Yılmaz), Ayrıntı Yayınları, İstanbul.

BECK Ulrich (2011). *Risk Toplumu: Başka Bir Modernliğe Doğru* (Çev. Kazım Özdoğan ve Bülent Doğan), İthaki Yayınları, İstanbul.

BİLGEHAN A. Deniz (2025). "Siber Güvenlik Başkanlığının Düzenlenişine Dair Değerlendirme", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 12:1, 63-88.

BİTİRİM OKMEYDAN Selin. (2017). "Postmodern Kültürde Gözetim Toplumunun Dönüşümü: 'Panoptikon'dan 'Sinoptikon' ve 'Omniptikon'a", *AJIT-e: Academic Journal of Information Technology*, 8:30, 45-69.

CASTELLS Manuel (2008). *Ağ Toplumunun Yükselişi* (Çev. Ebru Kılıç), İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

CLARKE Ronald V., ve CORNISH Derek B. (1985). "Modeling Offenders' Decisions: A Framework for Research and Policy", *Crime and Justice*, 6, ss. 147-185.

COOMBS W. Timothy (2022). *Ongoing Crisis Communication: Planning, Managing, and Responding*, 6. Baskı, Sage Publications, Florida.

CROWLEY David ve HEYER Paul (2019). *İletişim Tarihi* (Çev. Berkay Ersöz), Siyasal Kitabevi, Ankara.

ÇAKIR Hüseyin ve TAŞER Murat (2023). "Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi", *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, 11:2, 347-366.

ÇELİK Soner (2018). "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *ARHUSS,* 1: 2, 110-119.

ÇETİN Ebru (2016). "Kitle İletişim Aracı Olarak İnternet ve Hukuk İlişkisi: Türkiye Örneği", *Sosyoloji Dergisi*, 33, 1-13.

DARICILI Ali Burak (2019). "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli İçin Öneriler", *TESAM Akademi Dergisi*, 6:2, 11-33.

DELEUZE Gilles ve GUATTARI Félix (1987). *A Thousand Plateaus: Capitalism and Schizophrenia*, University of Minnesota Press, Minneapolis.

EFE Ahmet (2017). *Bilişim Suçları ve Türk Ceza Hukukundaki Yeri*, Seçkin Yayıncılık, Ankara.

ELDEM Tuba, (2021). "Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik", İstanbul Hukuk Mecmuası, 79: 1, 347-378.

ERDEM Merve ve Gürkan ÖZOCAK (2019). "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 68:1, 127-212.

ERGÜN İsmail (2008). *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Adalet Yayınevi, Ankara.

FLORIDI Luciano (1999). "Information Ethics: On the Philosophical Foundation of Computer Ethics", *Ethics and Information Technology*, 1, 37-56.

FOUCAULT Michel (1992). *Hapishanenin Doğuşu* (Çev. Ali Yaşar Kılıçbay), İmge Kitabevi Yayınları, Ankara.

GÖLE Nilüfer (1986). *Mühendisler ve İdeoloji* (Çev. Eli Levi), İletişim Yayınları, İstanbul.
GÜNDÜZ Muhammed Zekeriya ve DAŞ Resul (2020). "Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik", *Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 10:2, 970-984.
HABERMAS Jurgen (2001). İletişimsel Eylem Kuramı (Çev. Mustafa Tüzel), Kabalcı Yayıncılık, İstanbul.
HABERMAS Jurgen (1984). *The Theory of Communicative Action* (Çev. Thomas McCarty), Beacon Press, Boston.
HABERMAS Jurgen (1987). *The Theory of Communicative Action, Volume Two: Lifeworld and System: A Critique of Functionalist Reason* (Çev. Thomas McCarty), Beacon Press.
HABERMAS, Jurgen (1989). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Çev. Thomas Burger), MIT Press, Cambridge.
HABERMAS Jurgen (1991). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Çev. Thomas Burger ve Frederick Lawrence), MIT Press, Cambridge.
HABERMAS Jurgen (1996). *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (Çev. William Rehg), MIT Press, Cambridge.
HABERMAS, Jurgen (2006). "Political Communication in Media Society: Does Democracy still Enjoy an Epistemic Dimension?", *Communication Theory*, 16:4, 411-26.
HATİPOĞLU AYDIN Fatma (2023). *Siber Güvenlik ve Kişisel Verilerin Korunması: Hukuki Bir Değerlendirme*, Adalet Yayınevi, Ankara.
HEIDEGGER Martin (1977). *The Question Concerning Technology and Other Essays*, Harper & Row, New York.
JENKINS Henry (2006). *Convergence Culture: Where Old and New Media Collide*, New York University Press, New York.
KARASOY H. Alpay ve BABAOĞLU Pelin (2021). "Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı", *Yasama Dergisi*, 44, 123-155.
KARCI Reyhan (2023). "Ulusal Hukukta Kişisel Verilerin Korunması Hakkına İlişkin İstisnai Haller", Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy (Ed.), *Kişisel Verilerin Korunmasına Uzman Bakışı*, KVKK Yayınları, Ankara, 243-302.
KARTAL Pınar ve IŞIKLAR ALPTEKİN Gülfem (2023). "Türk Ceza Hukukunda Bilişim Sistemine Girme Suçuna İlişkin Değerlendirmeler", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 29:1, 16-31.
LOADER Brian D. ve THOMAS Douglas (2000). *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, London.
LUHMANN Niklas (1996). *Social Systems*, Stanford University Press, Stanford.
NEZGİTLİ Sena ve Recep BENZER (2020). "Avrupa Birliği Siber Güvenlik Kanunu", *Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi*, 2:1, 10-17.
NİŞANYAN Sevan (2022). *Nişanyan* Sözlük Çağdaş Türkçenin Etimolojisi, Liberus, İstanbul.
ÖNAL Mehmet Alperen (2021). "Siber Uzay Ve Güvenlik İlişkisi Bağlamında Siber Güvenliğin Boyutları", *Hitit Ekonomi ve Politika Dergisi*, 1:2, 114-23.
ÖZDEMİR Gülşah (2025). "Uluslararası Güvenlikte Siber Tehditlerin Yükselişi ve Stratejik Savunma Politikaları", *Elektronik Sosyal Bilimler Dergisi*, 24:1, 1-20.
POMERANTSEV Peter (2021). *Bu Propaganda Değil Gerçeğe Karşı Savaş Maceraları* (Çev. Alain Matalon), Mundi Kitap, İstanbul.
RAWLS John (2017). *Bir Adalet Teorisi* (Çev. Vedat Ahsen Coşar), Phoenix Yayınevi, Ankara.
RAWLS John (1971). *A Theory of Justice*, Harvard University Press, Cambridge.
SCHNEIER Bruce (2004). *Secrets and Lies: Digital Security in a Networked World*, New York: Wiley.
SHANNON, Claude E. (1948). "A Mathematical Theory of Communication", *Bell System Technical Journal*, 27:3, 379-423, https://archive.org/details/bstj27-3-379
SOLOVE Daniel J. (2007). *Understanding Privacy*, Harvard University Press, Cambridge.
TANENBAUM Andrew S. ve BOS Herbert (2015). *Modern Operating Systems*, Pearson, New Jersey.
TBMM (2020). *Türkiye Cumhuriyeti Anayasası*, TBMM Basımevi, Ankara.
The Council of Europe (2021). *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, The Council of Europe Publishing, Strasbourg.
Türk Dil Derneği (2012). *Türkçe Sözlük*, Türk Dil Derneği, Ankara.
Türk Dil Kurumu (2005). *Türkçe Sözlük*, 10. Baskı, 2., Türk Dil Kurumu, Ankara.
VOLKMAN Ernest (2004). *Casusluk* (Çev. Sevde Kubilay ve Melike Atik), Truva Yayınları, İstanbul.
WALL David S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge.

WIENER Norbert (2019). *Cybernetics or Control and Communication in the Animal and the Machine*, 3. Baskı, MIT Press, Cambridge.

YILDIRIM Arzu (2024). "Türkiye'nin Siber Güvenlik Politikasının Eylem Planları Üzerinden Analizi", *Organizasyon ve Yönetim Bilimleri Dergisi*, 16:1, 23-47.

YILMAZ Onur (2018). "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik", *Cyberpolitik Journal*, 4, 22-43.

ZUBOFF Shoshana (2018). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York.

İnternet Kaynakları

BIÇAKCI Salih ERGUN Doruk ve ÇELİKPALA Mitat (2015).*"Türkiye'de Siber Güvenlik"*, Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM) Siber Politika Kâğıtları Serisi 1, İstanbul, https://edam.org.tr/wp-content/uploads/2015/12/EDAM_TR_Siber_Guv_1.pdf, erişim 16.05.2025.

Bilgi Teknolojileri ve İletişim Kurumu (2025). "Siber Güvenlik Kurulu", *Bilgi Teknolojileri ve İletişim Kurumu*, https://www.btk.tr/siber-guvenlik-kurulu, erişim 15.08.2025.

ÇINAR Enes (2025). "Bilişim Suçları", Çınar Hukuk Bürosu, https://www.cinarhukukburosu.com/blog/bilisim-suclari, erişim 11.05.2025.

ÇAKIRCA Ege ÇAKIRCA Tuna ve ÇELİK Oylum (2025). "Türkiye'de Siber Güvenliğin Yeni Yasal Çerçevesi: 7545 Sayılı Siber Güvenlik Kanunu", *Turkish Law Blog*, https://turkishlawblog.com/insights/detail/turkiyede-siber-guvenligin-yeni-yasal-cercevesi-7545-sayili-siber-guvenlik-kanunu, erişim 15.08.2025.

DAĞISTANLI Hüseyin Cem ve SARICA Abdullah (2025). "Cumhurbaşkanlığına bağlı ofis ve politika kurullarına ilişkin düzenlemeler Resmi Gazete'de", *Anadolu Ajansı (AA)*, https://www.aa.com.tr/tr/gundem/cumhurbaskanligina-bagli-ofis-ve-politika-kurullarina-iliskin-duzenlemeler-resmi-gazetede/3522186, erişim 15.08.2025.

Siber Suçlarla Mücadele Daire Başkanlığı (2025). "Siber Suç Nedir?", *Emniyet Genel Müdürlüğü (EGM)*, https://www.egm.gov.tr/siber/sibersucnedir, erişim 16.05.2025.

ESEN SAKAR Gözde NART Ece ve ÜSTÜNDAĞ Pelinsu (2025). "7545 Sayılı Siber Güvenlik Kanunu", *Mondaq*, https://www.mondaq.com/turkey/security/1606732/7545-say%C4%B1l%C4%B1-siber-g%C3%BCvenlik-kanunu, erişim 15.08.2025.

European Data Protection Supervisor (2013). *Opinion of the European Data Protection Supervisor on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, European Data Protection Supervisor (EDPS), https://www.edps.europa.eu/sites/default/files/publication/13-06-14_cyber_security_en.pdf, erişim15.08.2025

Govinsider (2025). "Digital Transformation Office (DTO) of the Presidency of the Republic of Türkiye", *Govinsider*, https://govinsider.asia/intl-en/digital-government/country/turkey?utm_source=chatgpt.com&type=info&agency=digital-transformation-office-dto-of-the-presidency-of-the-republic-of-turkiye-80, erişim 15.08.2025.

Millî İstihbarat Teşkilatı (2025). "Yetki ve Sorumluluklar", *Millî İstihbarat Teşkilatı*, https://www.mit.gov.tr/yetki-ve-sorumluluklar.html, erişim15.08.2025.

STINE Kevin M. QUILL Kim ve WITTE Gregory A. (2014). "Framework for Improving Critical Infrastructure Cybersecurity", *National Institute of Standards and Technology*, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity, erişim 20.05.2025.

The Council of Europe (2021). *Guide on Article 10 of the European Convention on Human Rights*, The Council of Europe Publishing, Strasbourg, https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/11/Guide_Art_10_ENG.pdf?utm, erişim 10.05.2025.

The Council of Europe (1950). *European Convention on Human Rights*, The Council of Europe Publishing, Strasbourg, https://www.eods.eu/library/CoE_European%20Convention%20for%20the%20Protection%20of%20Human%20Rights%20and%20Fundamental%20Freedoms_1950_EN.pdf?utm, erişim 19.05.2025.

The Council of Europe (2003). *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*, The Council of Europe Publishing, Strasbourg, https://rm.coe.int/168008160f, erişim 15.08.2025.

Türkiye Büyük Millet Meclisi (2004). *Basın Kanunu*, Kanun No. 5187, https://www.resmigazete.gov.tr/eskiler/2004/06/20040626.htm, erişim 16.05.2025.

Türkiye Büyük Millet Meclisi (2008). *Elektronik Haberleşme Kanunu*, Kanun No. 5809, https://resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm, erişim 15.05.2025.

Türkiye Büyük Millet Meclisi (2007). İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Ed*ilmesi Hakkında Kanun*, Kanun No. 5651, https://resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm, erişim 16.05.2025.

Türkiye Büyük Millet Meclisi (2016). *Kişisel Verilerin Korunması Kanunu*, Kanun No. 6698, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf, erişim 15.05.2025.

Türkiye Büyük Millet Meclisi (2025). *Siber Güvenlik Kanunu*, Kanun No. 7545, https://resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm, erişim 13.05.2025.

Türkiye Büyük Millet Meclisi (1991). *Türk Ceza Kanunun Yürürlükten Kaldırılmış Hükümleri, 767 Mülga 765 sayılı Türk Ceza Kanunu On Birinci Bab Bilişim Suçları*, ss. 106-122., https://mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf, erişim 15.05.2025.

United Nations (2011). *"Article 19: Freedoms of Opinion and Expression"*, United Nations Human Rights Committee, https://www.refworld.org/legal/general/hrc/2011/en/83764?utm, erişim 18.05.2025.

United Nations (1967). *"International Covenant on Civil and Political Rights (ICCPR)*", United Nations Treaty Series, https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf?utm, erişim 18.05.2025.

Ulusal Siber Olaylara Müdahale Merkezi (2014). *"Siber Güvenliğe İlişkin Temel Bilgiler", Ulusal Siber Olaylara Müdahale Merkezi (USOM/TR-CERT)*, Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı, Ankara, https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf, erişim 15.05.2025.

Ulusal Siber Olaylara Müdahale Merkezi (2025). *"Hakkımızda/About Us"*, Ulusal Siber Olaylara Müdahale Merkezi, https://www.usom.gov.tr/hakkimizda, erişim 15.08.2025.