

AIHM İÇTİHADINDA EGEMENLİK, KARŞI-KAMUSALLIK VE EKOSİSTEM MEKÂNI OLARAK SİBER ALAN

Cyber Public Space as a Locus of Sovereignty, Counter-Publicness and Ecosystem in the ECtHR Jurisprudence

Zülfiye YILMAZ YAMAÇ*

Özet

Siber alanın ulus-devletlerin ülke unsurunun 21. yüzyıldaki uzantısı ya da yeni bir egemenlik alanı olarak tanımlanması çabaları yanında; özgürlük alanı, küresel müşterek statüsü, özel mülkiyete konu edilebilirliği ve nihayet *sui generis* yapısı nedeniyle heterotopya mekânı olarak da tasnif edilmesi, karşımıza zengin bir disiplinlerarası literatür çıkarmaktadır. Bunda siber alanın devletler, uluslararası kuruluşlar ve diğer devlet-dışı aktörler tarafından düzenlenmesi girişimleri etkindir. Bu çalışma kapsamında, siber alanın bir kamusal alan olduğu kabul edilerek hukukunun interdisipliner bir akademik incelemeye tabi tutulması hedeflenmektedir. Bu minvalde siber kamusal alan; egemenlik, karşı-kamusallık ve ekosistem mekânı olarak mercek altına alınacaktır. Her üç model siber alanın düzenlenmesinde, egemenlik tesisi ve insan haklarının korunması bakımından, dijital dünyanın sunduğu imkânlar ve yarattığı sorunlara yeni ya da siber alana uyarlanmış standartlar geliştirme çabasıdır. Hukuk ve diğer disiplinlerin siber alana dair tanımlarının uzlaşma ve çatışma kapasiteleri ise Avrupa İnsan Hakları Mahkemesi içtihadı ekseninde test edilecektir. İnsan haklarının siber alanda tabi olduğu kısıntılar ve korumaya dair yeni standartlar, Avrupa İnsan Hakları Sözleşmesi sisteminin siber alana nüfuz etme kapasitesini de ortaya koyacaktır.

Anahtar Kelimeler: Siber alan, egemenlik, karşı-kamusallık, ekosistem, insan hakları

Abstract

In addition to the endeavours to identify cyberspace in the realm of sovereignty as the final frontier of the nation-states in the 21st century, the classification of cyberspace as a space of freedom, a global common, private property or even as a locus for heterotopia due to its *sui generis* structure has yielded a rich interdisciplinary literature. The plethora of definitions can be attributed to the rigorous regulatory efforts on the part of the states, international organisations and other non-state actors. The objective of this study is to undertake an interdisciplinary academic interpellation of the law of cyberspace, operating under the assumption that cyberspace constitutes a public sphere. In this respect, the cyber public sphere will be analysed from a triangular approach based on sovereignty, counter-publicness and ecosystem models. It is evident that all three models are oriented towards the development of standards for the cyber governance in order to establish sovereignty in cyberspace and to protect human rights within. The repercussions of three models

➤ Bu makale Etik Kurul iznine tabi değildir/This article is not subject to Ethics Committee permission.

➤ Makale Geliş Tarihi/Article Received Date: 10.06.2025

➤ Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 22.07.2025

* Dr. Öğr. Üyesi, İhsan Doğramacı Bilkent Üniversitesi Hukuk Fakültesi Anayasa Hukuku Bölümü, zulfiye.yilmaz@bilkent.edu.tr, <https://orcid.org/0000-0001-9568-6372>

will be traced in the jurisprudence of the European Court of Human Rights. The embedding constraints in cyberspace, alongside the emerging standards for human rights protection in the Court's jurisprudence, will also demonstrate the (cyber)adaptive capacity of the Convention system.

Keywords: Cyberspace, sovereignty, counter-publicness, ecosystem, human rights

GİRİŞ

20. yüzyılın sonu ve içinde bulunduğumuz çağ, hukuk disiplininin ve özelde insan hakları hukukunun sürekli gelişen teknolojinin ortaya çıkardığı sorunlara yanıt vermesini talep etmektedir. Anayasalar ve insan hakları sözleşmelerinin yaşayan belgeler olması; dijital dünyada egemenliğin, hak ve özgürlüklerin ve bunlardan sadır sorumluluğun da yaşayan ve sürekli yeniden tanımlanan dinamik bir içeriğe sahip olmasını gerektirmektedir. Öte yandan anayasacılığın, hukuk devletinin ve demokrasinin krizlerinin süreklileşmesi karşısında, hukuk yoluyla bu dinamik alanı düzenlemek her zamankinden daha zorludur. Bu nedenle, dijital teknolojilerin ulus-devletin unsurları, ulusal ve uluslararası hukuk, egemen erklerin işlevleri ile insan hakları üzerinde yarattığı etki, kurucu bir anayasal moment olarak tanımlanmaktadır. Dijitalleşmenin özel hukuk etkisini yoğun biçimde kamu hukuku ve dahi anayasa hukuku alanına taşıması, anayasal norm ve ilkeler, temel haklar ve denge-denetleme kavramlarının kapsam ve işlevinin yeniden tanımlanmasını gerektirmesi bu tezin dayanağıdır.¹ Anayasal politikaların halkın kamusal tartışmalara yoğun ilgi göstermesini sağlayan siyasi hareketlerle şekillendiğini ve nihayetinde başarı elde ettiklerinde bunun halk adına üstün, bağlayıcı kurallara dönüştüğünü söyleyen Ackerman; anayasal momentin geleceği bakımından, hezimet ya da hukuka dönüşme olarak iki ihtimal olduğunu söylemektedir.² Siber alanın hukukunun düzenlemesi için siyasi, ekonomik ve hukuki alandaki çabaların gideceği yön de bu bağlamdan arı değildir.

William Gibson'ın 1984 tarihli *Neuromancer* adlı bilim kurgu kitabında; matematiksel kavramlar öğretilen her ulustan çocuğun deneyimlediği 'rızaaya dayalı halüsinasyon' fenomenine ve 'insan sistemindeki bilgisayarlardan soyutlanmış verilerin grafik temsili' kavramına atıfla ilk kez tasvir edilen³ siber alanın tanımı üzerinde halen bir uzlaşşı yoktur. Ancak fiziki kamusal alan ile siber alanı birbirine bağlayan altyapısal unsurları baz alan şu tanım yol gösterici olabilir: Siber alan; bilgisayar ve elektromanyetik dalgalardan oluşan, bilgisayar ağlarını kullanarak veri depolamak, değiştirmek ve değiş tokuş etmek üzere işlev gören, fiziksel ve

¹ Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33[1] *International Review of Law, Computers & Technology* 76-99. Hartzog ve Richards, özel yaşam ve mahremiyet ('privacy') düzenlemeleri ile veri koruma rejiminin tetiklediği toplumsal tartışma nedeniyle ABD özelinde mahremiyet rejiminin bir anayasal moment içinde olduğunu ileri sürmektedir. Bkz. Woodrow Hartzog and Neil M. Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection', (21) *Boston College Law Review* 1687- 1761.

² Bruce Ackerman, *We The People: Foundations* (Harvard University Press 1991) 7.

³ William Gibson, *Neuromancer* (Ace Book (Ebook 1984) Bölüm I.

fiziksel olmayan bileşenlerin oluşturduğu ortamdır. Unsurları ve işlevi sürekli yeniden tanımlanan dinamik siber alan yalnızca internette oluşmaz. Elektrik şebekeleri, su tedarik sistemleri, bankacılık işlemleri ve ulaşım sistemleri gibi kritik altyapıyı da kapsamaktadır.⁴

Öte yandan siber alanın hukuken düzenlenebilirliği noktasında Lessig; 1998⁵ ve 2006⁶ tarihli iki eserinde bazı uyarılarda bulunmuştu: Gerçek dünyada insan davranışlarının düzenlenmesi; hukuk kuralları, toplumsal kurallar, piyasa gerekleri ve mimari yapı dediği mekânsal sınırlılıklar ekseninde gerçekleşir. Gerçek dünyanın mimari/mekânsal sınırlamaları siber alanda koda dönüşür. Fiziki dünyanın düzenleyici kuralları olan anayasalar, siber alanda koda tabi bir *Lex Informatica*'dır. Kod, hem mekân hem hukuktur. Bu durum, siber alanın dinamikleri ve aktörleri yoluyla konvansiyonel hukuka meydan okuması ve onu teknolojinin, politikanın, ekonominin ve oluşturduğu yeni toplumsallığın etkisine maruz bırakması olarak tanımlanmaktadır.⁷ Hukuk gözünden siber alanın fiilen anayasadan arındırılmış bölge ('constitutional free cyberspace')⁸ olup olmayacağı sorusuna verilen yanıtlar muhtelif ve çoğunlukla olumsuzdur. Siber alanın devletlerin ülke unsurunun bir uzantısı, eş deyişle dijital ikizi olup olmadığı, bir küresel müşterek olup olarak tanımlanıp tanımlanmayacağı ya da başlı başına bir heterotopya alanı⁹ niteliği tartışmaları devam etmektedir. Ancak şu gerçektir ki siber alandaki çok aktörlü egemenlik yarışı, Westphalia tipi egemenlik anlayışının fiili egemenlik yetkisi teorisi ('extra-territorial jurisdiction') ile dahi nüfuz edilemeyen dinamikler barındırmaktadır.

Bu çalışma kapsamında, siber alanın bir kamusal alan olduğu kabul edilerek hukukunun interdisipliner bir akademik incelemeye tabi tutulması hedeflenmek-

⁴ Andrew N. Liaropoulos, 'Cyberspace Governance and State Sovereignty' in George C. Bitros and Nicholas C. Kyriazis (eds), *Democracy and an Open-Economy World Order* (Springer 2017) 25-35.

⁵ Lawrence Lessig, 'The Laws of Cyberspace', <https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf> erişim tarihi: 25.03.2025.

⁶ Lawrence Lessig, *Code Version 2.0* (Penguin 2006) 1-28.

⁷ Duygu Hatipoğlu Aydın, *Siber Alan ve Hukuk* (On İki Levha 2022)137-170.

⁸ Paul S. Berman, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to 'Private' Regulation' (2000) (71) *University of Colorado Law Review* 1271.

⁹ Heterotopik mekânlar; kurgusal, ütöpik mekânlardan farklı ilkelere tabidir. Tekil bir fiziki alanı birbirleriyle muhtemelen uzlaştırılamayacak farklı mekânlarla bağlantılandırması, fiziki mekânlardaki zaman senkronizasyonunu kırması, geleneksel kamusal alan gibi izinsiz, herkese açıklık ilkeleri karşısında onay ya da inisiyasyon ritüellerini gerektirebilmesi, insan yaşamının yanılsamalara dayalı mekânsal ve gündelik işleyişini gün yüzüne çıkaran bir illüzyon mekânı yaratması ya da gerçek mekânı mükemmelleştiren diğer mekân olarak işlev görmesi; modern hukukun belirlilik, öngörülebilirlik ve denetlenebilirlik vaatlerinin yarattığı güven duygusunu sarstığı gibi toplumsal ihtiyaçlara yanıt veren dinamik yapısının sınırlarını da teste tabi tutmaktadır. Michel Foucault, 'Des espaces autres Hétérotopies' (1967) <https://historiacultural.mpbnet.com.br/pos-modernismo/Des_espaces_autres.pdf> erişim tarihi:15.03.2025.



tedir. Bu minvalde siber kamusal alan; egemenlik alanı, karşı-kamusallık alanı ve ekosistem olarak mercek altına alınacaktır. Hukuk ve diğer disiplinlerin siber alana dair tanımlarının uzlaşma ve çatışma kapasiteleri ise Avrupa İnsan Hakları Mahkemesi (AIHM-Mahkeme) içtihadı doğrultusunda test edilecektir. Böyle bir yol izlenmesinin nedeni, siber alanın hukukunun yalnızca hukuk kuramı ekseninde şekillenmemesi ve teknik, ekonomik ve siyasi dinamiklerin hukukileştirme yoluyla normatif çerçeveye dahil edilmesidir. Bu doğrultuda, öncelikle siber alanda egemenlik sorunsalı ele alınacak ve ardından içtihatındaki egemenlik ve Avrupa kamu düzeni kavramlarının siber alana içkin meselelere nüfuz kabiliyeti irdelenecektir. Ardından Habermas'ın liberal-burjuva kamusal alan tezine karşı Fraser tarafından ileri sürülen karşı-kamusallık ('counterpublicness') tezinin siber alana uyarlanabilirliği incelenecektir. Son bölümde bir ekosistem olarak siber alan tezine odaklanılacaktır. Ekosistem yaklaşımı; aktörler, dinamikler ve yaygın etki bakımından siber alana bütüncül bakışı salık vermektedir. Her üç yaklaşımda insan haklarının korunması bakımından Avrupa İnsan Hakları Sözleşmesinin (AIHS-Sözleşme) denetiminde kullanılan araçların siber alana uyarlanması ve kısıntılarına odaklanılarak çalışma tamamlanacaktır.

A. AVRUPA KAMU DÜZENİ KAVRAMI EKSENİNDE SİBER ALANDA EGEMENLİK

Siber alanın modern egemenlik kuramının mekânı olmadığını söyleyen Barlow, 1996'da siber alanı özgürlük ve kendi kaderini tayin ekseninde biçimlenen, her yerde ve hiçbir yerde olan bir yer olarak tanımlamıştı.¹⁰ Ancak geline nokta, devletler arası dijital egemenlik yarışı, siber operasyonların sınır aşan etkisi¹¹ ya da insan haklarının etkili korunması gibi hedeflerle uluslararası hukuk, uluslararası insan hakları hukuku ve insancıl hukuk ilkelerinin siber alanda uygulanması için girişimler söz konusudur.

Siber alanın modern ulus-devletlerin ülke unsurunun 21. yüzyıldaki bir görünümü ya da Westfalyen anlayışta 'Devlet'i oluşturan unsurlarla açıklanamayan 'yeni' bir egemenlik sahası olarak tanımlanma çabası¹², esasında Westphalia sonrası ulus-devletlerinin yaslandığı rasyonel yönetilebilirlik ('gouvernabilité') ilkesinin yansımasıdır. Yönetilebilirlik, toprak üzerinde bölünmüş egemenliği merkezileştiren ulus-devletin, rasyonellik hattı ekseninde toprağı ve nüfusu ön-

¹⁰ John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (1996) <<https://www.eff.org/cyberspace-independence>> erişim tarihi: 11.02.2025.

¹¹ 2000-2025 arasında, veri hırsızlığı ('theft, doxing ya da hijacking yöntemleri ile'), hizmetlerin aksatılması ('disruption'), fidye yazılımlar ('ransomware') yoluyla, devletler, devlet bağlantılı gruplar ya da devlet dışı aktörler tarafından, politik ya da diğer amaçlarla gerçekleştirilen 3656 siber olay ('cyber incident') tespit edilmiştir. Bkz. European Repository of Cyber Incidents, 'Cyber Incident Dashboard (2024)' <<https://eurepoc.eu/dashboard/>> erişim tarihi: 04.05.2025.

¹² Thanos Koulos, 'A digital territory to be appropriated: the state and the nationalization of cyberspace' (2022) *Open Research Europe*.

görülebilir ve kontrol edilebilir bir rejimde yönetme arzusunun *telosunu* oluşturmaktadır.¹³ Bu nedenle siber alan, fiziksel alanın bir tür dijital ikizi muamelesi görebilmektedir Dijital ikiz; gerçek dünyadaki süreçleri ya da sistemleri simüle etmek üzere tasarlanmış dijital replikalardır. Yapay zekâ, robotik, büyük veri, nesnelerin interneti ('IoT') ve diğer dijital teknolojiler aracılığıyla, sistemlerin ve toplumların gelecek dizaynında işlev görmesi beklenen dijital ikizler; siber alanda ayrıntılı simülasyonlar ve veri odaklı öngörüler sağlayan, fiziksel dünya ile siber alanı birbirine bağlayan köprü niteliğindedir.¹⁴

Farklarına rağmen uluslararası hukuk düzleminde, siber alanda adeta bir dijital hukuk ikizi yaratılmaya çalışıldığını söylemek mümkündür. 2017 tarihli Tallinn Kılavuzu,¹⁵ Birleşmiş Milletler Genel Kurulunun 31 Aralık 2020 tarihli kararı,¹⁶ Avrupa Birliği Konseyinin 18 Kasım 2024 tarihli deklarasyonu/pozisyon belgesi¹⁷ bunun somut örneğidir. Uzmanlar bildirgesi¹⁸ niteliğindeki Tallinn Kılavuzu dışında yumuşak hukuk ('soft law') belgeleri olan bu metinler; siber alanda devletlerin ülkesel/teritoryal egemenliğinin uygulama alanını, insan haklarının korunması yükümlülükleri kapsamında devletlere atfedilebilir ('attributable') sorumluluğun kapsamını ve egemenlikten sadır yargı yetkisinin ('jurisdiction') sınırlarını belirlemeye çalışmaktadır.

Bunlar arasında en yakın tarihli metin olan Avrupa Birliği Konseyi pozisyon belgesinde vurgulanan ilkelere baktığımızda, siber alanın hukuku şu şekilde tanımlanmaktadır: Siber alanda uluslararası hukuk, uluslararası insan hakları hukuku ve insancıl hukukun uygulanması; devletlerin egemen eşitliği, müdahale yasağı, özen yükümlülüğü, kuvvet kullanımının yasaklanması ilkelerini gündeme getirecektir. Egemen yargı yetkisi kuralları, bilgi iletişim teknolojileri kapsamında bir devletin ülkesel egemenlik sahasındaki altyapı unsurları ve siber faaliyetlerde bulunan kişiler bakımından siber alana uyarlanacaktır. Bir devletin

¹³ Michel Foucault, *Dits et Ecrits* (Gallimard 1994) 232-237 Tome IV.

¹⁴ Roberto Saracco, 'Digital Twins: Bridging Physical Space and Cyberspace' (2019) 52 [12] *Computer* 58-64; Tokio Takada, Jin Nakazato, Alex Orsholits, Manabu Tsukada, Hideya Ochiai and Hiroshi Esaki, 'Design of Digital Twin Architecture for 3D Audio Representation in AR' (2024) 2024 *IEEE International Conference on Metaverse Computing, Networking, and Applications* 222-230.

¹⁵ Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017). *Bundan sonra ilgili metne, 'Tallinn Kılavuzu (n 15)' olarak atıf verilecektir.*

¹⁶ Developments in the Field of Information and Telecommunications in the Context of International Security (UN General Assembly Resolution 31 December 2020) <<https://digitallibrary.un.org/record/3896180?ln=en>> erişim tarihi:12.02.2025

¹⁷ Declaration on a Common Understanding of International Law in Cyberspace (Council of European Union, 18 November 2024) <<https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/>> erişim tarihi:14.02.2025.

¹⁸ Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 [4] *American Journal of International Law* 583-657.



toprak bütünlüğüne müdahale ya da hükûmet işlevine içkin fonksiyonlarını bozma ya da ele geçirmeye neden olan başka bir devlete atfedilebilir siber faaliyetler; klasik anlamda yasaklanmış müdahale ve kuvvet kullanma biçimlerinden birini oluşturmada da, siber alanda uluslararası hukuka aykırı fiil olarak tanımlanabilecektir. Özen yükümlülüğü; devletlerden ya da devlet dışı aktörlerden sadır siber aktiviteler yoluyla bir başka devletin haklarının ihlalini engellemek üzere bütün gerekli, makul olarak erişilebilir ve elverişli önlemlerin alınması yükümlülüğünü siber alana taşıyacaktır. Bu nedenle, devletin kendi yetki sahası içinde ya da sınır ötesinde etkili kontrolü altındaki altyapı dahil sistemlerde siber aktiviteleri izlemesi, özen yükümlülüğünün gereğidir. Gündelik yaşamın büyük ölçüde bilgi ve iletişim teknolojilerine bağlı olarak gerçekleştiği modern yaşamda, kamu hizmetlerine erişimin bozulduğu ya da engellendiği durumlarda, fiziksel bir hasar olmasa da gündelik yaşam üzerindeki etkisi ve ölçeğine bağlı olarak bu faaliyetler bir tür kinetik kuvvet kullanma olarak değerlendirilebilecektir. Bu da meşru savunma hakkını doğurabilecektir. Devletlerin haksız fiilden kaynaklanan uluslararası hukuk sorumluluğuna ilişkin ARSIWA¹⁹ ilkeleri ekseninde, devlet dışı aktörlerden sadır hukuka aykırı siber aktivitelerden bir devletin sorumlu tutulabilmesi, devlet adına hareket ya da bu hukuka aykırı fiillerin devlet tarafından onaylanması ya da benimsenmesi halinde gündeme gelebilecektir.

1. Egemenlik, Avrupa Kamu Düzeni ve Sorumluluğun Sınırları

Egemenlik ilkesi yukarıdaki çerçeveye göre devletlerin yetki alanının sınırlarının belirlenmesinde rol aldığı gibi insan haklarının tanınması, korunması, gerçekleştirilmesi ve ilerletilmesi bağlamında bir hukuk boşluğunun doğmasını da engellemeye yönelik işlev görmektedir. Nitekim Avrupa İnsan Hakları Sözleşmesinin (AİHS-Sözleşme) 1. Maddesi, egemenlik yetkisi altındaki herkes bakımından Sözleşmedeki hak ve özgürlükleri güvence altına alınması (‘to secure’) yükümlülüğü getirmektedir. Mahkemenin yargı yetkisinin belirlenmesinde de dikkate alınan bu madde; Sözleşmeye taraf devletin, haklarının ihlal edildiğini ileri süren kişinin bulunduğu yer ya da bölgede etkili kontrol sağlaması (‘spatial model of jurisdiction’) ya da yetkilendirdiği kişilerce haklarının ihlal edildiğini ileri süren kişi üzerinde otorite ya da kontrol sağlanması (‘personel model of jurisdiction’) halinde sözleşmesel sorumluluğunu gündeme getirmektedir.²⁰ Dahası Mahkeme, fiili egemenlik (‘extra-territoriality’) kavramı yoluyla devletlerin insan hakları ihlallerinden kaynaklı sorumluluğu ve haliyle kendi yargı yetkisinin sınırlarını da genişletmiştir. Bu da bizi Mahkeme içtihadındaki bir diğer kavram

¹⁹ International Law Commission’s Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA 2001) <https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf>erişim tarihi: 22.01.2025.

²⁰ Marko Milanovic, ‘Jurisdiction, Attribution and Responsibility in Jaloud’ (EjilTalk 2014) <<https://www.ejiltalk.org/jurisdiction-attribution-and-responsibility-in-jaloud/>>erişim tarihi:23.03.2025.

olan Avrupa kamu düzeni ('European public order') doktrininin teritoryal ve fonksiyonel işlevini incelemeye sevk edecektir.

1960'ta Lawless/İrlanda (1)²¹ kararında, karşı oyda dillendirilen Avrupa düzeni kavramı, 1 yıl sonra Avusturya/İtalya²² kararında, taraf devletlerin ulusal çıkarlarından öteye geçen, özgür demokrasilerden oluşan Avrupa'da siyasi gelenekler, idealler, özgürlük ve hukuk devletinin korunması hedefini içeren bir ortak kamu düzeni hedefi olarak tanımlanmıştır. Sonraki kararlarında ise Mahkemenin yargı yetkisi, Mahkeme ve diğer uluslararası örgütler arası diyalogun esasları,²³ kabul edilebilirlik koşullarının belirlenmesi,²⁴ demokrasinin korunması²⁵ ile Sözleşme-deki hak ve özgürlüklerin norm alanının belirlenmesinde Mahkemenin yetkisi²⁶ kapsamında bir Avrupa kamu düzeni çerçevesi oluşmuştur. Öte yandan Avrupa kamu düzeni doktrinine Mahkemenin ve dahi AİHM yargıçlarının bakışı tutarlı değildir. Kavramın ilintili olduğu hukuki-siyasi değerlere dair yapılan bir çalışmaya göre bazı yargıçlar; hukuk devleti, kuvvetler ayrılığı, çekirdek hakların gardiyanı olarak Mahkemenin rolü, anayasa hukukundaki sonsuzluk hükümlerine benzer işlevin AİHS düzeyine taşınması, Avrupa konsensüsünün ve ayrıca transnasyonel ve küresel eğilimlerin tespiti²⁷ gibi fonksiyonel işleve gönderme yaparken diğerleri kavramın muğlak ya da fazla esnek olduğunu belirtmiştir.²⁸

Devletlerin egemen sınırları dışındaki faaliyetleri nedeniyle gündeme gelen insan hakları ihlallerinde sorumluluk bağını inşa etmek üzere başvurulanan fiili egemenlik ('extra-territoriality') kavramı, Avrupa kamu düzeni yaklaşımının hakların korunmasına yönelik fonksiyonel işlevinin simgesidir.²⁹ Loizidou/Türkiye kararından³⁰ bu yana ve ayrıca Viyana Andlaşmalar Hukuku Sözleşmesinin 31(3)(c) kuralı gereği Mahkeme; AİHS'in bir vakum içerisinde değil; uluslararası hukuk kurallarının ışığında uygulanacağını vurgulamaktadır. 2001 tarihli Banković ve

²¹ AİHM, Lawless/İrlanda (1), B. No. 332/57, K.T. 14/11/1960.

²² AİHM, Avusturya/İtalya, B.No. 788/60, K.T.11/01/1961, s.18.

²³ AİHM, Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi/İrlanda (B.D.), B. No. 45036/98, K.T. 30/06/2005 § 156.

²⁴ AİHM, De Becker/Belçika, B. No. 214/56, K.T. 27/03/1962, §25.

²⁵ AİHM, Türkiye Birleşik Komünist Partisi ve Diğerleri/Türkiye, B. No. 19392/92, K.T. 30/01/1998, §45.

²⁶ AİHM, De Wilde, Ooms ve Versyp/Belçika, B. No. 2832/66, K.T. 18/06/1971.

²⁷ AİHM, Dániel Karsai/ Macaristan, B. No. 32312, K.T. 13/06/2024, Karşı Oy, § 5.

²⁸ Kanstantsin Dzehtsiarou, *Can the European Court of Human Rights Shape European Public Order?* (Cambridge University Press 2022) 22-61.

²⁹ Samantha Besson, 'The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to' (2012) (25)[4] *Leiden Journal of International Law* 863.

³⁰ AİHM, Loizidou/Türkiye (B.D.), B. No:15318/89, K.T. 18/12/1996, § 43.



Diğerleri/Belçika ve Diğerleri³¹ ve 2011 tarihli Al-Skeini ve Diğerleri/Birleşik Krallık³² kararlarıyla açtığı yolda, egemenlik yetkisi kullanımının tanımı, kapsamı ve sonuçları bakımından Avrupa kamu düzeninin alanını ve bu alanda insan haklarının korunması bakımından uygulanabilecek çerçeveyi belirlemeye çalışmıştır. Banković kararında, Avrupa kamu düzeninin anayasal enstrümanı olarak Sözleşmenin denetim mekanizması Mahkemenin, Sözleşmenin 19. Maddesi doğrultusunda taraf devletlerin taahhütlerini yerine getirip getirmediğini denetlemek üzere kurulduğu ve fiili egemenlikten kaynaklı sorumluluğun denetiminin de bu kamu düzeninin parçası olduğu vurgulanmıştır. Al-Skeini kararında ise taraf devletlerin kontrol ve denetimi altındaki kişiler bakımından sorumluluk, durumun koşullarına göre Sözleşmedeki hakların tek tek belirlenmesi ('The Convention rights can be 'divided and tailored') ekseninde tayin edilecektir (Para. 137). Bu iki kararın yön verdiği hatta; devletin ülkesi dışında etkin denetim sağladığı alanlarda ya da etkin kontrol sağlanmadığı durumlarda dahi, *de facto* hükümet etme yetkileri doğrultusunda devlet organlarının kişiler üzerinde talimat ve denetim yoluyla kontrol sağlamaları veyahut da konsolosluk ve diplomatik organları yoluyla egemenlik yetkisi kullanımı halinde, Sözleşmeden kaynaklı yükümlülüklerin doğurduğu sorumluluk ileri sürülebilecektir. Dahası, 2021 tarihli Hanan/Almanya kararı doğrultusunda, taraf devletin ülkesi dışında ve ordusu aracılığıyla dahil olduğu bir hava saldırısında ölen kişilerin ölümlerinin iç hukukta soruşturulması yükümlülüğü, Sözleşmenin 2. Maddesinde korunan yaşam hakkının usuli boyutu üzerinden, Mahkemenin soruşturmadaki ihmalleri denetleme yargı yetkisinin dayanağını oluşturmuştur. AIHM, bu bağın kurulmasının ('jurisdictional link'), yaşam hakkının ihlalini getiren fiillerin devletin egemenlik alanında gerçekleştiği ya da ona atfedilebilir olduğu anlamında yorumlanamayacağını da vurgulamıştır (Para.134-145). Bu karar, etkin kontrolün olmadığı ya da hükümet etme yetkileri doğrultusunda talimat ve denetim yoluyla kontrol sağlanmadığı hallerde dahi sözleşmesel hak ve menfaatler üzerinde kontrolü ('control over the rights doctrine')³³ olan ülkelerin sorumluluğunun gündeme gelebileceğini göstermektedir³⁴. Arsava'ya göre; Banković'ten Al-Skeini kararına gelen çizgi bakımından ortak amaç, Sözleşmedeki hakların korunmasında Avrupa hukuki

³¹ AIHM, Banković ve Diğerleri/Belçika ve Diğerleri (B.D.), B. No. 52207/99, K.T.12/12/2001, § 80.

³² AIHM, Al-Skeini ve Diğerleri/ Birleşik Krallık (B.D.), B. No.55721/07, K.T. 07/07/2011, §141.

³³ Başak Çalı, 'Has 'Control over Rights Doctrine' for Extra-territorial Jurisdiction Come of Age? Karlsruhe, too, has Spoken, Now It's Strasbourg's Turn' (EjilTalk 2020) <<https://www.ejiltalk.org/has-control-over-rights-doctrine-for-extra-territorial-jurisdiction-come-of-age-karlsruhe-too-has-spoken-now-its-strasbourgs-turn/>> erişim tarihi: 11.04.2025.

³⁴ Benzer yönde Carter/Rusya kararında AIHM; geçmişte Rusya Federal Güvenlik Servisinde çalışan bir üst düzey görevlinin, Birleşik Krallık'ta Rusya'nın talimatı ile Rus görevlilerce öldürülmesi iddiasına dair başvuruda; Rusya makamlarının kendi soruşturmasını yürütmesi ve Birleşik Krallık makamlarıyla iş birliği konusundaki tutumu ekseninde 2. Maddenin usuli boyutunun ihlaline karar vermiştir. Bkz. AIHM, Carter/Rusya, B. No. 20914/07, K.T. 21/09/2021 § 133-148.

kamusal alanında ('legal space/espace juridique') boşluk doğmasının engellenmesidir.³⁵ Hanan kararı bu hattın devamı sayılabilecektir. Ancak güncel gelişmeler, Avrupa kamu düzeninin yersel ve fonksiyonel işlevinin AİHM tarafından yeniden şekillendirildiği izlenimi vermektedir. 2024 tarihli Duarte Agostinho ve Diğerleri/Portekiz ve Diğerleri kararında³⁶, Hanan kararının aksine, ne yaşayan belge yaklaşımının ne de kararın konusunu oluşturan iklim krizinin yıkıcı etkisi ve acil önlem gereğinin, Sözleşmenin 1. Maddesindeki yargı yetkisinin genişletilmesine imkân vermediğini belirtmiştir. Oysa sözleşmesel menfaat ve haklar üzerinde kontrol testi yerine, sözleşmesel hakların gerçekleştirilmesini engelleyen, sınır aşan etkiye sahip riskli faaliyetlerin ülkesel kontrolü bağlamında bir değerlendirme, Mahkemenin konvansiyonel egemenlik-fiili egemenlik yaklaşımlarına daha uygun olabilirdi.

Yukarıdan bu yana çizilen hat, devletlerin siber alandaki faaliyetler nedeniyle kişiler ve diğer devletlere karşı insan hakları sorumluluklarının kapsamının belirlenmesinde de işlev görecektir. Bu noktada siber alanda faaliyet gösteren devlet dışı aktörlerin faaliyetlerinin devletlere atfedilmesinin imkânı da yanıtlanması gereken bir diğer sorudur. Doktrindeki bir görüşe göre; devlet dışı aktörün bir devletin iç hukuku uyarınca hükûmet etme yetkisi kapsamında otorite kullandığı; devletin talimatı ile hareket ederek bir başka devletin güvenliği zayıf/kırılğan altyapı unsurlarına zarar vermek üzere operasyon yaptığı, devletin operasyonu onama veya iptal gibi doğrudan kontrolü söz konusu olduğu veyahut devletin sonradan operasyonu onayladığını kamuya duyurması halinde, sorumluluğun taraf devlete atfedilmesi mümkün olacaktır. Bunlar dışında, devlet bir isyancı gruba kötü yazılım ya da eğitim sağlıyorsa veya siber operasyonlarda altyapı-

³⁵ Füsün A. Arsava, 'AİHK'nun Extraterritorial Geçerliliği Bağlamında AİHM'nin İçtihatlarında Görülen Hareketlilik' (2019) (25)[2] *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 590-601.

³⁶ *AİHM*, Duarte Agostinho ve Diğerleri/Portekiz ve Diğerleri (B.D.), B.No. 39371/20, K.T.09/04/2024 §82-83. Esasında Mahkeme burada dile getirilen sorunun farkındadır ve iklim krizi bağlamında ve fiili egemenlik teorisi doğrultusunda devletlerin sorumluluk alanının somut davada neden genişletilemeyeceğine dair bir gerekçelendirme çabası içerisindedir. Buna göre; bir devletin kontrolü altındaki kamu ya da özel kişilerin faaliyetlerinden kaynaklı sera gazı emisyonlarının iklim üzerindeki olumsuz ve sınır aşan etkisi, başvuruçuların Sözleşmeden kaynaklanan menfaatlerinin ihlali argümanını beraberinde getirmiştir. Ancak başvuruçuların uğradığı zarar ile bu faaliyetler arasındaki illiyet bağına kurmak, bunların zamansal ve mekânsal etkilerini tespit etmek zorludur ve aynı zamanda devletlerin sınırları dışındaki faaliyetlerinden kaynaklanan sözleşmesel sorumluluğunun kapsamının aşırı genişlemesine neden olabilecektir. AİHS'in amaç ve kapsamının ve bunlardan sadır egemenlik ve yargı yetkisi yaklaşımının, BM İklim Değişikliği Çerçeve Sözleşmesi gibi konuya özgü uluslararası hukuk metinlerinden ya da andığı diğer uluslararası denetim mekanizmalarının yaklaşımlarından farklı olduğunu belirten Mahkeme; bir devletin kontrolü altındaki riskli faaliyetlerin neden olduğu sınır aşan zarar iddiasının, somut olay bakımından başvuruçuları riskli faaliyetlerin yürüttüğü devletin egemenlik sahasındaki kişilere karşı sorumluluğu ile eş değer bir konuma taşımayacağını söylemiştir (Bkz. Para.205-212). Devletlerin karbon emisyonları üzerindeki kontrol yetkisine dayanarak yargı yetkisini temellendiren örnek karar için Bkz. *BM Çocuk Hakları Komitesi*, Chiara Sacchi ve Diğerleri/ Arjantin, B. No: 104/2019, K.T.23/09/2021, §10.

sını kullanıyorsa ve tarafsız davranmıyorsa ve bu yüzden başka bir devletin egemenlik alanına müdahale ediliyorsa, devletlerin sorumlu olması gerektiği belirtilmektedir.³⁷

Ancak siber alanın fiziksel katmanı üzerinde kontrol sağlanamadığı ya da dijital teknolojilerin yardımıyla faaliyetlerini gizleyerek gerçekleştiren devlet dışı aktörlerin fiilleri nedeniyle devletlere sorumluluk atfının zorluğu bakidir.³⁸ Dahası Mueller; devletlerin fiziksel altyapıya gönderme yaparak siber alanda egemenlik iddiaları ile sorumluluktan kaçmak için siber alanın sınırsızlığı ve kontrolsüzlüğü tezlerini eş zamanlı ileri sürmesini çelişkili bulmaktadır. Yazara göre; siber kapasitenin cebri kullanımı; kod, ağlar, bilgi işlem cihazlarının bulunduğu ve internet protokollerinin bunlar arasında iletişimi sağladığı her yerde ve her anda mümkündür. Bu alanda devletler ve devlet dışı aktörler arasında ayrım yoktur.³⁹ Liaropoulos ise büyük platformlar, alt yapı sağlayıcılar veya üçüncü kişiler olarak tanımladığı devlet dışı aktörlerin siber alandaki imtiyaz ve etkisinin, siber alanın bir egemenlik sahası olarak tanımlanmasını engellediğini savunmaktadır.⁴⁰ Bununla birlikte yeni *Leviathan*lar olarak adlandırılan büyük teknoloji şirketlerinin, devletlerin sağladığı hizmetlerde teknolojik altyapı sağlaması, ürünler yoluyla hizmetin sunulmasına aracılık etmesi, hizmetin bilfiil sunumu gibi işlevleri üstlenmesi nedeniyle, devletlerden devlet dışı aktörlere *de facto* bir egemenlik transferinin söz konusu olduğu ve haliyle bunların faaliyetlerinden doğan sorumluluğun devletlere atfedilebileceği de dillendirilmektedir.⁴¹

2. Örnek AIHM Kararları

Mahkemenin A. A ve Diğerleri/Makedonya kararında,⁴² yasadışı göç gibi kontrol edilmesi zor durumlarda, devletlerin insan hakları ihlallerindeki sorumluluklarını bertaraf etmek üzere ileri sürdükleri etkin kontrol yokluğu argümanını kabul etmemiştir. Buna göre taraf devlet, hiçbir zaman ihlalin gerçekleştiği alandaki egemen yetkilerinden vazgeçmemiştir. Kamu gücü kullanan makamların yasa dışı göç kapsamındaki kişilere ilişkin geri gönderme gibi idari tasarrufları⁴³ da bunun

³⁷ Michael N. Schmitt and Sean Watts, 'Beyond State-Centrism: International Law and Non-state Actors in Cyberspace' (2016) (21)[2] *Journal of Conflict & Security Law* 600-606.

³⁸ Berkant Akkuş, 'Devletin Etkin Kontrolünün Bulunmadığı Siber Alanda İnsan Hakları Yükümlülükleri Nelerdir?' (2024) (6)[1] *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi* 168-171.

³⁹ Milton Mueller, 'Against Sovereignty in Cyberspace' (2020) (22)[4] *International Studies Review* 790.

⁴⁰ Liaropoulos (n 4) 25-35.

⁴¹ Hongfei Gu, 'Data, Big Tech, and the New Concept of Sovereignty' (2023) (29) *Journal of Chinese Political Sciences* 596-612.

⁴² AIHM, A.A ve Diğerleri /Kuzey Makedonya, B.No. 55798/16, K.T. 05/04/2022, § 62-63.

⁴³ AIHM'in Mansouri/İtalya kararında, çalışma iznine tabi olarak İtalya'da yaşayan ve oturma izni biten bir kişinin, İtalyan bir şirkete ait gemi tarafından limanda inmesine izin verilmemesi ve geri gönderilmesi olayı söz konusudur. İtalya, gemi kaptanının kamu görevlisi olmadığı argümanını ileri sürmüştür. Mahkeme ise kaptanın, idarenin sınırdan almama işlemini uygulamak zorunda

göstergesidir. Haliyle devletin toprak üzerindeki *etkili kontrolünü sınırlandıran de facto durumlar* ya da *objektif olgular* argümanı, yetki karinesini ('presumption of competence') bertaraf etmeyecektir. Taraf devletlerin Sözleşmeden kaynaklanan yükümlülüklerini seçtikleri egemenlik alanlarında uygulaması, devletin ülkesel egemenlik yetkisinde soyut bir zayıflatma ('artificial reduction') teşkil edeceğinden, göç olgusu, kişilerin hukukun korumasından yoksun bırakıldığı ve sözleşmesel haklardan faydalanamadıkları bir durumu gerektelendirmeyecektir.

Atıf yapılan soyut zayıflatma yasağı ve yetki karinesi, siber alanda ve siber alanla bağlantılı hak ihlallerinin engellenmesi ve onarımına yönelik devletlerin pozitif edim yükümlülüklerinin de dayanağı olabilecektir. Ancak S.S. ve Diğerleri/İtalya⁴⁴ kararı ile bu argümanın geçerliliği Mahkemece zayıflatılmıştır. Başvuruda, açık denizden İtalya kıyılarına yaklaşan Libya kalkışlı bir göçmen botunun yardım çağrısı sinyalinin İtalyan makamları tarafından tespiti sonrasında meydana gelen insan hakları ihlallerinden sorumluluk incelenmiştir. 2012 tarihli Hirsi Jamaa ve Diğerleri/İtalya⁴⁵ kararında, taraf devletlerin açık denizde insan hakları sorumluluğunun çerçevesini çizen Mahkeme, göçmenleri Libya makamlarına teslim etmek üzere operasyona dahil olduğunu iddia eden İtalyan makamlarının, başvuruçular üzerinde *de jure* ve *de facto* etkin kontrolünün varlığını kabul etmiştir. S.S. ve Diğerleri kararında ise İtalyan makamları yardım sinyalinin tespit edip bu kez doğrudan müdahale için Libya makamlarına haber vermiştir. İki ülke arası göç kontrolü anlaşması gereğince İtalya, Libya'ya teknik ve teknolojik destek sağlamaktadır. Aralarında çocukların da bulunduğu 150 kişinin çoğunun öldüğü olayda Mahkeme; özerk hareket ettiğini belirttiği Libya makamları üzerinde İtalyan makamlarının etkin kontrolünün olmadığını, uluslararası sularda gerçekleşen olayda İtalya'nın, yer ('ratione loci') bakımından ya da ihlale uğrayan başvuruçular ('ratione personae') ile başvuruçuların sözleşmesel hakları ('control over the rights doctrine') üzerinde etki doğuran uluslararası hukuka aykırı fiiller bakımından sorumluluğunu tesis edecek delil sunulmadığını belirterek kabul edilemezlik kararı vermiştir. Bu karar; teknolojik araçların giderek daha yaygın kullanıldığı sınır kontrolü uygulamaları sonucunda meydana gelen ihlallerde, devletlerin insan haklarını koruma sorumluluğunun kapsamını ve geleceğini düşünmek bakımından iyi bir örnektir. İleri teknolojilere sahip devletlerin göç alanında kontrolü elinde tutarken, uygulamayı ve haliyle sorumluluğu diğer ülkelere ya da devlet-dışı aktörlere açık ya da zımni devri ('outsourcing'), Sözleşmenin 1. Maddesinin ve dahi Sözleşme düzeninin işlevsizleşmesine neden olmamalıdır. Zira mevcut durumda ve göç olgusu özelinde, Avrupa kamu düzeni

olduğunu ve İtalyan hukukuna göre kamu gücü kullanan makam sayıldığını vurgulayarak fiillerin devlete atfedilemezliği (ratione personae yetkisizlik) iddiasını reddetmiştir. Bkz. *AİHM*, Mansouri/İtalya (B.D.), B.No. 3386/16, K.T. 29/04/2025, §57-62.

⁴⁴ *AİHM*, S.S. ve Diğerleri/İtalya, B. No. 21660/18, K.T. 20/05/2025, §89-108.

⁴⁵ *AİHM*, Hirsi Jamaa ve Diğerleri/İtalya (B.D.), B. No. 27765/09, K.T. 23/02/2012, § 76-82.



doktrininin yersel işlevinin Avrupa sınırlarında genişlediğini ancak Avrupa sınırları dışındaki yersel ve fonksiyonel işlevinin ('extra-territoriality') daraldığını söylemek mümkündür.

Bir diğer örnek karar, istihbarat amaçlı kitlesel gözetleme ('bulk interception') politikaları ile ilgilidir. Çok sayıda devletin *amicus curiae* ('third party observations') yoluyla İsveç'e destek verdiği Centrum För Rättvisa/İsveç kararında⁴⁶ Mahkeme öncelikle, teknolojik kapasitenin artışıyla birlikte devletler ile vatandaşları bakımından ortaya çıkan tehditlerin (küresel terörizm, uyuşturucu ve insan kaçakçılığı, çocukların cinsel istismarı gibi) çeşitlendiğini vurgulamıştır. Sonrasında verilecek Big Brother Watch ve Diğerleri/Birleşik Krallık kararında⁴⁷ da benimsenecek ilkeler koyan Rättvisa kararına göre, devletler ve devlet dışı aktörlerin kullandığı teknolojik araç ve yöntemler, siber saldırılar yoluyla ulusal güvenliği etkileyebildiği gibi devletlerin egemenlik alanlarına yönelen yeni tehditleri tespit kapasitesi de sunmaktadır. Öte yandan kitlesel gözetlemenin gerekçesi olan ulusal güvenlik amacı, yalnızca dijital alanda ('digital domain') mevcuttur; haliyle ancak orada tespit edilebilir ve soruşturulabilir durumdadır. Mahkemenin yapacağı denetim bu nedenle, dijital alandaki keyfilik ve kötüye kullanıma karşı devletin aldığı önlemlerin Sözleşmeye uygunluğu ile sınırlıdır ve bu denetimi de taraf devletlerin kitlesel gözetleme rejimlerinin işleyişine dair kendisine sunduğu ya da Mahkemenin erişebildiği sınırlı bilgi ekseninde gerçekleştirecektir.

Mahkeme, Big Brother Watch ve Diğerleri Daire kararında⁴⁸, 8. Madde kapsamındaki hak ve özgürlüklere müdahalenin kapsamını da sınırlandırmıştır. Buna göre; yabancı istihbarat makamları tarafından gerçekleşen istihbari amaçlı iletişimin izlenmesi faaliyetlerinin kendisinin, Birleşik Krallık'ın yetkisi dahilinde ya da ona atfedilebilir olduğunu söylemek mümkün değildir; zira taraf devletin yabancı istihbarat birimleri üzerinde otorite ya da kontrolü yoktur. Haliyle Birleşik Krallık'ın Sözleşme kapsamında sorumlu olduğu müdahale, kitlesel izleme yoluyla yabancı kuruluşlar tarafından elde edilen materyalin 'alınması', 'depolanması', 'incelenmesi' ve 'kendi istihbarat servisleri tarafından kullanılmasından' ibarettir (Para.420). 1. Maddeye dair Birleşik Krallık tarafından herhangi bir itiraz getirilmemesine rağmen, Mahkemenin devletin sorumlu olduğu müdahalenin kapsamını sınırlaması ve kitlesel izleme faaliyetlerinin başlı başına Sözleşmeye aykırı olmadığını sıklıkla vurgulaması nedeniyle, bu faaliyetlerin Avrupa kamu düzeni içerisinde insan haklarının korunması standardına etkisi dikkatle izlenmelidir.

Nitekim 2024 tarihli bir başka kararında, Birleşik Krallık vatandaşı olan ve cezaevinde bulunan 2 kişi tarafından, veri depolama merkezi Fransa'da bulunan

⁴⁶ AIHM, Centrum För Rättvisa/İsveç, B. No. 35252/08, 25/05/2021, §237.

⁴⁷ AIHM, Big Brother Watch ve Diğerleri/B.K (B.D.), B.No. 58170/13, K.T. 25/05/2021.

⁴⁸ AIHM, Big Brother Watch ve Diğerleri/B.K (1. Daire), B.No. 58170/13, K.T. 13/09/2018. Daire kararına ayrıca atıf yapılmasının nedeni, Büyük Daire kararında, Daire kararındaki 1. Madde değerlendirmesine atıfla yetinilmesi ve dikkat çekilen konuya ayrıca değinilmemesidir.

ve 122 ülkede faaliyet gösteren EncroChat şifreli mobil telefon kayıtları sistemi verilerinin Fransa tarafından Birleşik Krallık'a aktarımının 8. Madde kapsamında yasal müdahale ilkesini ihlal ettiği ileri sürülmüştür.⁴⁹ Mahkeme bu olayda, verilerin Fransa'da toplandığını ('captation') ve depolandığını dikkate alarak, Fransa'nın yargı yetkisini kabul etmiş ve kişi bakımından yetkisizlik argümanını reddetmiştir. Öte yandan ilgili verilerin Avrupa Soruşturma Talimatı ('European Investigation Order') kapsamında delil olarak Birleşik Krallık'a aktarıldığını, başvuruçuların kişisel veri aktarım işlemine karşı Fransa'daki etkili onarım yollarına başvurmadığını ve dahası bu yolla ulusal makamların veri aktarımı konusundaki içtihadını geliştirmesine *fırsat tanımadıkları* ('*Les juridictions internes ont ainsi été privées de la possibilité de développer leur jurisprudence sur la question*') belirterek başvuruyu kabul edilemez bulmuştur.

Siber alanda gerçekleştirilen fiiller bakımından, Mahkeme içtihadında uygulama alanı bulabilecek bir başka kavramın etki doktrini ('effects doctrine') olduğu savunulmaktadır.⁵⁰ Rekabet hukuku çıkışlı bir kavram olan etki doktrini, farklı egemenlik alanlarından geçen ya da kaynağı ve güzergahı tespit edilemediği için sözleşmesel denetimi bertaraf edebilecek fiiller bakımından, yardım veya destek olarak tanımlanabilecek uluslararası hukuka aykırı davranışlarda sorumluluk atfına imkân vermesi nedeniyle desteklenmektedir. Etki doktrininin gündeme gelmesi; ABD, Çin ve Avrupa Birliği'nde⁵¹ dijital teknolojiler ve siber alan düzenlemele-
rinin hukuk alanındaki yansıması olarak adlandırılmaktadır. Bignami ve Resta, digital alanı düzenleme modellerini ihraç etmeye çalışan bu 3 aktörün yaklaşımının siber alanın hukukunun geleceğini belirleyeceğini belirtmektedir. Haliyle, politik ve ekonomik modellerin hukukileştirilmesi eğilimi somuttur. Her 3 örnekte ortak olan ise düzenlemeler ya da fiili uygulamalar yoluyla, etki doktrini ve fiili egemenlik yetkisi yaklaşımı aracılığıyla egemenlik alanının genişletilmesi amacıdır.⁵² Tallinn Kılavuzunu hazırlayan uzmanlar, devletlerin etki doktrinini esas alarak ekonomik aktiviteler ve hukuk düzeninin işleyişini sekteye uğratan siber aktiviteleri yasaklayan ya da cezalandıran düzenlemeler yapabileceğini; ancak bu mevzuatın belirli koşulları taşıması gerektiğini vurgulamıştır. Bu minvalde; düzenleyici devletin açık ve uluslararası kabul edilebilir bir menfaatinin olması,

⁴⁹ *AIHM*, A.L. ve E.J./Fransa, B. No. 44715/20, K.T. 24/09/2024, §104, 145.

⁵⁰ Diego Mauri, 'On American Drone Strikes and (Possible) European Responsibilities: Facing the Issue of Jurisdiction for 'Complicity' in Extraterritorial Targeted Killings' (2019) (28) [1] *The Italian Yearbook of International Law*, 249-272.

⁵¹ Avrupa Birliği'nde internet düzenlemeleri ve Dijital Hizmetler Yasası ('Digital Services Act') özelinde egemenlik kavramını ele alan çalışma için Bkz. Alper Işık, *İnternet Aktörleri ve Egemenliğin Değişen Boyutları: Digital Services Act ve Türk Mevzuatı Özelinde Bir İnceleme* (On İki Levha 2025, 2.Baskı) 115-120.

⁵² Francesca Bignami and Giorgio Resta, 'Extraterritoriality' in Giovanni De Gregorio, Oreste Pollicino, and Peggy Valcke (eds), *The Oxford Handbook of Digital Constitutionalism* (online edn, Oxford Academic 2024).



düzenlemeyi hedeflediği etkilerin yeterince doğrudan, kasıtlı ve öngörülebilir olması, bu etkilerin devletin kendi hukukunu sınırları dışındaki yabancı kişilere doğru genişletmesini gerektirecek nitelikte önemli olması ve etki doktrinine dayalı egemenlik/yargı yetkisi kullanımının diğer devletlerin ya da üçüncü kişilerin menfaatlerini haksız yere ihlal etmemesi gereklidir.⁵³ Ancak etkiye maruz kalan devletlerin yargı yetkisini ileri sürmesi; yargı yetkisi çatışmasına ya da hakkaniyet ilkesinin ihlalini de gündeme getirebilecektir.⁵⁴ Devlet otoritesinin her yerdeliği ('ubiquity') iddialarına neden olabilecek etki doktrinin gündeme getirilmesi eleştirilmekte⁵⁵ ve siber alanda uygulanabilirliğinin imkân dahilinde olmadığı da belirtilmektedir. Haliyle bu doktrinin siber alan hukuku üzerindeki doğrudan ve/veya dolaylı etkisinin izlenmesi gerekecektir.

Bir sonraki bölümde egemenlik tartışmaları karşısında karşı-kamusallık mekânı olarak siber alanın hukukuna ilişkin tartışmalara yer verilecektir.

B. KARŞI-KAMUSALLIK MEKANI OLARAK SİBER KAMUSAL ALAN

*'Devlet ile toplum arasında kamusal alan vardır. Bu kamusal alan, 18. yüzyıldan bu yana ulus-devlete özgü dinamikler ekseninde sürekli olarak devinim halindedir; sabit bir formatı yoktur. Özel kişilerin bir kamusal beden oluşturmak üzere bir araya geldiği bu kamusal alan, müzakere yoluyla kamuoyu oluşturmada işlev görmektedir. Özel kişiler bu alanda, ne ticari amaçlarla ne de anayasal düzenin bürokratik kurallarla çerçevelenmiş aktörleri olarak bulunurlar. Kamusal alana erişimde tüm vatandaşlar bakımından bir serbesti söz konusudur ve bu anlamda kamusal alan kapsayıcıdır. Siyasi kamusal alan ise devlet işlerine özgü tartışmaların alanıdır. Kamunun bilgiye erişim yoluyla sağladığı siyasi denetim sayesinde, siyasi kamusal alan, yönetim üzerinde kurumsallaşmış bir etki gücü kazanabilir. İlk modern anayasalar, temel haklar katalogları sayesinde burjuva kamusal alanı ile özel alan arasındaki sınırları çizmiştir. Ancak Sanayi Devrimiyle birlikte, refah devletine dayalı hak talepleri özel kişilerin bir araya geldiği, müzakere yoluyla oluşan kamuoyu esasını sarsmıştır. Devlet, emek ve meta değişim ilişkilerine müdahale ederken, toplumsal güçler de siyasi işlevler edinmiştir. Bu aşamadan itibaren burjuva kamusal alanının yeniden feodalleşmesi diyebileceğimiz bir süreç başlamıştır...'*⁵⁶

Jürgen Habermas'ın yukarıdaki çerçeve ile özetlenen burjuva kamusal alanı tezi, Avrupa kamu düzeni kavramının esası ve sınırları bakımından önem arz

⁵³ Tallinn Kılavuzu (n 15) 9-176.

⁵⁴ Nicholas Tsagourias, 'The Legal Status of Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Elgar Online 2021) 20.

⁵⁵ Cedric Ryngaert, 'Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts' (2023) (24)[3] *German Law Journal* 537-550.

⁵⁶ Jürgen Habermas, 'The Public Sphere: An Encyclopedia Article' Çev. Sara Lennox, and Frank Lennox (1974) (3) *New German Critique* 49-55.

etmektedir. Bireylerin yurttaşla dönüştüğü, katılım yoluyla toplumsal normlara ve kararlara dahil olduğu söylemsel kamusal alan diskuru karşısında, bu alanın hegemonik rıza üreten bir mekâna dönüşebilme potansiyeli, siber alanın özgürlük-egemenlik ekseninde gördüğü işlev bakımından da sorgulanmalıdır. Liberal kamusal alana getirilen eleştiriler⁵⁷ ve somut olarak Nancy Fraser tarafından teorize edilen karşı-kamusal ya da madun kamusal alan (‘subaltern counter-publics’) tezi,⁵⁸ siber alanda devletler ile devlet dışı aktörler aracılığıyla belirlenen erişim, düzenleme ve hak koruma standartlarının muhatapları bakımından da bir değerlendirme imkânı sunmaktadır. Zira siber kamusal alan, tıpkı burjuva kamusal alanında olduğu gibi herkese ve her düşünceye açık değildir ve müzakereci esası da zayıftır.

Fraser; Habermas’ın teorize ettiği liberal kamusal alanın açıklık ve müzakere yoluyla kamuoyu oluşturma idealinin, esasında baştan beri dışlayıcı olduğunu ileri sürmektedir. Buna göre; liberal kamusal alanın özgür tartışma yoluyla hesap verebilirlik sağlama mottosunun, kamu-özel çıkarlar ayrımı yoluyla politik tahakkümü rasyonelleştiren bir yanı vardır. Oysa kamusal alana çıkabilen fikirler ve öznelerin eşitliği ve bunların serbestçe ve ortak yarara dayalı müzakeresi pratikte mümkün değildir. Bir başka husus ise burjuva ya da liberal olmayan alternatif ya da yarışan kamusal alanların varlığının yok sayılmasıdır. Liberal kamusal alan fikri, müzakere eden bir sivil toplum ve karar veren bir devlet aygıtı tasarlayarak aslında zayıf kamusalılığı (‘weak publics’) topluma ve güçlü kamusalılığı (‘strong publics’) siyasal erklerle atfetmektedir.

Siber alanın özgürlük veya tahakküm yaratma potansiyelini anlamak için platform yanlılığı denilen ve algoritmalar yoluyla görünürlüğe yön veren, klasik kamusal alandaki ayrıcalıkları yeniden üreten ve hiyerarşi ekseninde madun kamusal alanları bölen bir tabakalanmayı da dikkate almak gerekir.⁵⁹ Sansür ve dezenformasyon, karşı- kamusal mekânını güç ilişkileri ekseninde şekillendiren en önemli araçlardır. Bir başka sorun ise devletler ve kişilerin dijital dünyanın imkânlarından yararlanmasında dijital uçurumun (‘digital divide’)⁶⁰ oluşturduğu bariyerdir. Nitekim AIHM Jankovskis/Litvanya kararında,⁶¹ internetin kamu hizmeti değeri (‘public service value’), haklara erişim ve hakların kullanılmasında araç niteliği ve bazı bilgilerin artık yalnızca internette olması nedeniyle, devletlerin

⁵⁷ Ülker Yükselbaba, ‘Kamusal Alan Modelleri ve Bu Modellerin Bağlamları’ (2011) (66)[2] *Journal of Istanbul University Law Faculty* 250-255.

⁵⁸ Nancy Fraser, ‘Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy’ (1990) (12) [25/26] *Social Text* 56-80.

⁵⁹ Victor Kempf and Sebastian Seignani, ‘Capitalism and Contested Publicity. A Conversation with Nancy Fraser’ (2023) (50)[1] *Philosophy & Social Criticism* 66-79.

⁶⁰ Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press 2001) 247-275.

⁶¹ *AIHM*, Jankovskis/Litvanya, B. No. 21575/08, K.T. 17/01/2017 § 62.

internete erişimde kimseyi geride bırakmadan ('universal access to the Internet') dijital uçurumu ortadan kaldıracak önlemler alması gerektiğini vurgulamıştır.

Bu yapısal sorunları göz ardı ederek siber alanda birey eksenli bir liberal özgürlük rejimi kurgulamak ya da bireysel haklarla sınırlı bir korumaya odaklanmak bu nedenle yetersizdir. Karşı-kamusallık bağlamında siber alan üzerine çalışmalar bu nedenle siber faaliyetlerin kolektif etkisine dikkat çekmektedir. Bu minvalde bireysel haklar yaklaşımı yanında bireylerin mensubu olduğu grupların özerkliğinin ve dahası mahremiyet haklarının sağlanması gereği dile getirilmektedir.⁶² Bunun nedeni ise büyük veri çağında bireysel verilerin nihai olarak grup dinamiklerini ve toplumsal eğilimleri öngörmeye yarayan kurucu işlevidir. Mevcut halde siber alanda kişisel verilerin korunması ve mahremiyet eksenli/insan onuru odaklı rejim öne çıkarken; kişisel ve kolektif verilerin korunması adına mülkiyet hakkı eksenli ve daha çok sözleşmeler hukukuna dayanan modeller de tartışılmaktadır. İnsan onuru temelli yaklaşımda, kişilerin aydınlanmış rızası olmaksızın verilerinin toplanması pratikleri nedeniyle, kişi özerkliği ve enformasyonel kendi kaderini tayin hakkının ihlal edildiği savlanmaktadır. Bu yaklaşım öte yandan, kişisel düzlem karşısında kolektif ve toplumsal boyutta ortaya çıkan sorunlara, siber alanda faaliyet gösteren ve dahası siber alanı düzenleyen devlet dışı aktörlerle kişiler arası yatay ilişkilerin hiyerarşik unsurlarına ve bunun demokratik işleyişe etkisine nüfuz edemediği için eleştirilmektedir.⁶³ Buradan yola çıkarak bütüncül bir yaklaşımın benimsenmesi ve bu doğrultuda siber alanda faaliyet gösteren aktörlerin ve siber süreçlerin denetimi,⁶⁴ hak ihlallerinin giderilmesi için etkili ve çift yönlü usuli güvenceler sisteminin kurulması; prosedürel özen yükümlülüğünün ('procedural due process') ve daha genelde hukuk devletinin gereği olarak tanımlanmaktadır.⁶⁵

AİHM içtihadında yukarıdaki görüşlerin izini sürdüğümüzde, bireysel ve kolektif etkinin birlikte değerlendirildiği örnekleri, karşı-kamusallık mekânı olarak siber alanın dışlayıcı ve/veya içerici dinamiklerini gözlemlemek mümkündür. Örneğin hükümet faaliyetlerini gözlemci ('watchdog') sıfatıyla izleyen ve bu nedenle yöneticileri geçmişte yaptırıma uğrayan bir hükümet dışı kuruluşun mensuplarının yaptığı Szabó ve Vissy/Macaristan başvurusunda⁶⁶ AİHM, gizli izlemeye ('secret surveillance') izin veren yasadan kaynaklı potansiyel mağdu-

⁶² Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017) 83-100.

⁶³ Salomé Viljoen, 'A Relational Theory of Data Governance' (2021) (131) [2] *Yale Law Journal* 623-634.

⁶⁴ Lisa M. Austin, 'Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)' in Austin Sarat (ed), *A World without Privacy: What Law Can and Should Do?* (Cambridge University Press 2014) 131-189.

⁶⁵ Margot E. Kaminski, 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2019) (92) *California Law Review* 1554.

⁶⁶ *AİHM*, Szabó ve Vissy/Macaristan, B.N. 37138/14, K.T. 12/01/2016, §34-40, 57.

riyet iddialarını kabul etmiştir. Yasal düzenlemeler, anti-terörizm kapsamında, özel polis kuvvetleri tarafından 180 güne kadar uzayan sürede istihbarat toplama faaliyetlerine izin vermektedir. Roman Zakharov/Rusya kararından⁶⁷ bir yıl sonra verilen bu kararda AİHM; başvuruçuların kişisel özellikleri ya da belirli bir gruba mensubiyetleri dolayısıyla mı söz konusu istihbari faaliyetlerin konusu haline geldiklerini, mevzuatın iletişim hizmeti kullanıcısı herhangi bir kişiyi doğrudan etkilemesi potansiyelini ve söz konusu faaliyetlerin siyasi ve hukuki denetiminin etkililiğini değerlendirmiştir. Yasanın lafzına göre, ‘bir yelpazede tanımlanan... ilgili kişiler’ (‘the notion of ‘persons concerned identified’ ... as a range of persons’) kavramı, herhangi bir kişinin izlenmesine neden olabilecektir. Usuli güvenceler bakımından sorunlu husus ise kişilere hiçbir zaman bildirim yapılmayacağı için bireysel başvuru gibi denetim mekanizmalarının işletilmesinin zorluğudur. Bu gerekçelere dayanan Mahkeme; yeni teknolojilerin, hükümetin başlangıçtaki operasyon alanı/amacı dışındaki kişilerle ilgili de büyük çaplı veriyi kolayca ele geçirmesine imkân tanıdığını vurgulayarak, 8. maddenin ihlal edildiğine hükmetmiştir. Zira, ulusal güvenliği korumak üzere kurulan gizli izleme sistemleri, çatışan değerler arasında adil denge kurulmadığında, bireysel-kolektif özgürlükler yanında, demokrasiyi koruma kisvesi altında demokrasiyi yok edebilecek pratiklere dönüşmeye de adaydır.

Ecodefence ve Diğerleri/Rusya kararında⁶⁸ AİHM, demokratik sürecin sürekli olarak özgür ve çoğulcu kamusal tartışma ile desteklenmesi gereğini ve sivil toplumun bundaki rolünü ele almıştır. Buna göre; ulusal güvenlik meşru amacı doğrultusunda sivil toplumun sınır aşan ya da uluslararası faaliyetlerinin denetim yoluyla sınırlandırılması, sadece tekil devletlerin değil; tüm taraf devletlerin ve dahası Avrupa Konseyinin meselesidir. Zira Avrupa kamu düzeninin ve *kolektif güvenliğin* enstrümanı olan Sözleşmede korunan değerler, Sözleşmenin yasal mekânındaki bütün insanların yararlanması gereken güvencelerdir. Bu nedenle damgalamaya neden olmayan bir çerçevede, öngörülebilir bir denetim rejimi kurulması halinde ancak baskın toplumsal ihtiyaç kriteri sağlanacaktır.

Bu iki karar, Mahkemenin bireysel düzlemde Avrupa ölçeğine doğru bir demokrasi standardı arayışında olduğunu göstermektedir. Ancak dijital teknolojiler yoluyla kolaylaşan siber faaliyetlerin kolektif etkisine dair yapacağı tartışmanın sözleşmesel kısıntıları da söz konusudur. Bunun en yakın örneği, Călin Georgescu/Romanya başvurusu⁶⁹ ile AİHM önüne de taşınan, Kasım 2024 Romanya Cumhurbaşkanlığı seçimlerinin Anayasa Mahkemesi tarafından iptalidir. Bağımsız aday Georgescu, seçim kampanyasını Tik Tok ve Facebook platformları üzerinden yürütmüş ve ilk tur seçimlerinde 2 milyondan fazla oy alarak ikinci

⁶⁷ AİHM, Roman Zakharov/ Rusya (B.D.), B. No. 47143/06, K.T. 04/12/2015, §§ 170-172.

⁶⁸ AİHM, Ecodefence ve Diğerleri/Rusya, B. No. 9988/13, K.T. 14/06/2022, §139.

⁶⁹ AİHM, Călin Georgescu/Romanya, B. No. 37327/24, K.T.11/02/2025, §21-36.



turda yarışmaya hak kazanmıştır. Bu evrede, Ulusal Yüksek Savunma Konseyi (CSAT); Tik Tok üzerindeki kampanyalarda, diğer devletler ve devlet-dışı aktörler tarafından siber saldırılar yoluyla seçim süreçlerine müdahale edildiğini raporlamıştır. Ayrıca isim vermeksizin adaylardan birinin Tik Tok kampanyaları yoluyla diğer adaylar karşısında daha fazla desteklendiğini ve seçim yarışının adilliği ilkesine zarar veren avantaj elde ettiğini açıklamıştır. Seçimlerin ikinci turu başladığında, diğer adayın seçimlerde düzensizlik iddiası ile AYM'ye başvurusu üzerine; önce birinci turun oylarının yeniden sayılmasına ve ardından seçimin bütünüyle iptaline karar verilmiştir. Kararda; seçmen iradesinin dijital teknolojiler ve algoritmalar yoluyla saptırılması, adaylara dair yanlış bilginin yayılması suretiyle avantaj elde etme, seçim harcamaları meblağı '0' (sıfır) olarak rapor edilen Georgescu'nun beyanlarının tutarlı olmadığı gerekçelerine dayanılmıştır. İptalin amacı; seçmenlerin korunması, adaylar arası adil yarışın güvencelenmesi ve demokratik hukuk devletinin uzantısı olan seçim ilkelerine saygının sağlanmasıdır.⁷⁰ AİHM; yasama seçimleri dışında kalan söz konusu seçimlere dair iddiaları konu bakımından yetkisizlik (P1-3) nedeniyle incelememiştir. Başvurucuya yöneltilen ithamların, 6. Madde kapsamında medeni hak ve yükümlülük ya da suç isnadı kapsamında olmadığı ve başvurunun ulusal makamlara yönelttiği iddiaların olgusal dayanakları sunulmadığı gerekçesiyle, başvuruyu açıkça dayanaktan yoksun bulmuştur.

Söz konusu uyumsuzluk ve karar; temsili demokrasilerde halkın siyasetal karar alma süreçlerine katılımının aracı olan seçimlerin dijital dünyadaki hukuki rejimi ve geleceği bakımından yeni tartışmaları beraberinde getirecektir. Dijital teknolojiler ve platformlar yoluyla kişilerin siyasi görüşlerinin ve daha özelde seçmen iradesinin bir tür *nöro-hackleme* pratiğine tabi tutulması⁷¹ ve bu pratiklerin seçim sonuçlarına etkisinin delillendirilmesinin ve haliyle ihlal ile siber faaliyetler arasında illiyet bağının kurulmasının zorluğu; ilk bölümde yer verilen egemenlik sahası olarak siber alanın barındırdığı hukuki sorunları, karşı-kamusal alan olarak siber alana da taşıyacaktır. Dahası siber alanın özgür propagandaya alan açan bir karşı-kamusallık mekânı ya da özgürlük illüzyonuna yaslanan bir hegemonya sahası olup olmadığı her somut olayda yeniden tanımlanacaktır. Haliyle AİHM'in seçimlere dair konu bakımından sınırlı yetkisi somut olayda esasa dair değerlendirme imkânı sunmasa da ileride yetkisi dahilindeki bir seçime yabancı devletler ve/veya devlet dışı aktörlerin müdahalesi iddia edildiğinde (bireysel ya da devletler arası başvuru yoluyla) devletlere atfedilebilir fiiller bağlamında yargı yetkisini nasıl somutlaştıracığı ve dijital dünyanın yarattığı yeni insan

⁷⁰ Irina Amaritei, 'Les élections présidentielles en Roumanie : la Constitution contre Tik-tok' (2024) *Questions Constitutionnelles: Revue de droit constitutionnel*.

⁷¹ Özgür düşünce ve kanaat hürriyeti bağlamında nöro hakların önemi için Bkz. Nora Hertz, 'Neurorights – Do We Need New Human Rights? A Reconsideration of the Right to Freedom of Thought' (2023) (16) [5] *Neuroethics*.

hakları ihlallerine Sözleşmenin yanıt verme kapasitesini nasıl şekillendireceği merak konusudur.

Karşı-kamusalılık başlığında dile getirilen meselelerden bir diğeri siber alana erişim, siber alanda görünürlük ile dijital uçurumun yarattığı kırılmanlık durumunun ortaya çıkardığı teknolojik bariyer ve eşitsizliklerdi. AİHM içtihadında bu başlığı, maddi eşitlikçi pozitif önlem ve usullere gönderme yapan *kırılmanlık* ('vulnerability') içtihadı ekseninde ele almak mümkündür. AİHM içtihadında, kırılmanlık durumunun kaynağına ve kişilerin psiko-kültürel durumlarına odaklanan yaklaşım yanında, grup ve kişi temelli, kesişimsel kırılmanlık tespitlerine rastlamak mümkündür.⁷² Bununla birlikte siber alandaki aktörlerin özel statüsünden bağımsız, alana özgü bir *içkin kırılmanlık* durumu söz konusudur. Zira ne siber alanın işleyiş dinamiklerine ne de gelişim hızı ve araçların çeşitliliğine nüfuz edebilecek bir teknolojik kapasiteye erişim mümkündür. Bu argüman, Fineman'ın insanlık durumuna içkin bir hal olarak kırılmanlık tanımına yaslanmaktadır. İnsan haklarının görünürdeki öznelerinin rasyonel, özgür ve özerk irade sahibi olması beklentisi, kırılmanlık durumunu istisnai olarak sunarken, esasında evrensel ve kaçınılmaz olan ve bu nedenle toplumun ve devletin sorumluluğunu gerektiren bir durumdur kırılmanlık.⁷³ Liberal kamusal alanın ve kamusal alandaki öznelerin eşitliği tezlerini alaşağı etme potansiyeline sahip içkin kırılmanlık durumu, insan haklarının soyut özneleri yerine gerçek yaşamdaki eşitsizlikleri ve haliyle toplumun ve kurumların da kırılmanlığını apaçık etme potansiyelini haizdir.

AİHM; Stichting Landgoed Steenbergen ve Diğerleri kararında,⁷⁴ Hollanda'da bir belediyenin web sitesinde ilan ettiği bir idari karardan haberdar olmadıkları için mahkemeye erişim haklarının ihlal edildiğini ileri süren başvuruclarının iddiaları incelenmiştir. Başvuruda, *amicus curiae* yoluyla bir sivil toplum kuruluşu, bilgi ve iletişim teknolojilerinin yaygınlığının, Hollanda'da vatandaşların e-katılımını yeterince güçlendirmedeğini ve dahası herkesin internet kullanmak zorunda olmadığını raporlamıştır. Mahkeme, Hollanda'da 12 yaş üstü nüfusun yüzde 92'sinin internete erişiminin olduğu ve 2011'den bu yana elektronik bildirim usulünün zorunlu ve hatta bazı hallerde tek yöntem olacağının yerel gazete ve televizyonlarda duyurulduğuna dair hükümet savunmasını dikkate almıştır. Hükümet ayrıca, başvuruclarının internet veya bilgisayara erişim sorunu yaşayan veya bilgisayar okuryazarlığı olmayan ve haliyle idari kararlara aydınlatılmış vatandaş katılımı sağlayamayan kırılman kişiler olmadığını savunmuştur. Bu savunma esasında ilginçtir. Zira Big Brother Watch ve Diğerleri/Birleşik Krallık

⁷² Corina Heri, *Responsive Human Rights: Vulnerability, Ill-treatment and the EctHR* (Hart Publishing 2021) 88-120.

⁷³ Martha A. Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2016) (20)[1] *Yale Journal of Law and Feminism* 8-14.

⁷⁴ AİHM, Stichting Landgoed Steenbergen ve Diğerleri/ Hollanda, B. No. 19732/17, K.T. 16/02/2021, § 39, 46-54.



(B.D) kararında, üçüncü taraf olarak müdahil olan Hollanda, kitlesel izleme araçlarının gerekliliği tezini, dijital teknolojilere dayanan idaresinin siber saldırılar karşısında kırılgan olduğu argümanına dayandırmıştı (Para.303). Oysa sistemler kırılgan iken vatandaşların kırılganlığının yalnızca internete erişimle giderilmesi pek mümkün değildir. AİHM ise işleyen ve erişilebilir bir idare kurmak adına, devlet ve vatandaşlar arasında elektronik iletişim yollarının seçiminin, çatışan menfaatlere neden olabileceğini kabul etmiştir. Başvurucuların bilgisayar ve internete erişimlerinin ya da bilgisayar okuryazarlıklarının olmadığına dair bir savunma yapmadıklarını belirten Mahkeme, devletin takdir yetkisini aşmadığını ve başvuruculara, söz konusu karara itiraz etme bakımından aşırı bir külfet yüklediğini belirterek 6. Maddenin ihlal edilmediğine hükmetmiştir. Ancak ilgili kararın açtığı yolda ve Sözleşmeye taraf devletlerin dijitalleşme eğilimlerini dikkate alarak Mahkemenin de içkin kırılganlık ve dijital yetkinlik ayrımı noktasında dikkatli olması gerekecektir. Zira internete erişimle sınırlı bir yetkinlik incelemesi, karşı-kamusallık alanında görünürlük ve hakların korunması bakımından yeni bir eşik oluşturabilecek; bazı (kırılgan) grupların Avrupa dijital kamu düzeninin koruma alanından dışlanmasına da neden olabilecektir.

Egemenlik ve/veya karşı-kamusallık mekânı olarak siber alan yaklaşımlarının barındırdığı sorunları aşmak üzere hukuki, teknik, politik çareler geliştiren ve aynı zamanda yeni sorunları gündeme getiren siber alana ekosistem yaklaşımı çalışmanın son uğrağı olacaktır.

C. SİBER KAMUSAL ALANA EKOSİSTEM YAKLAŞIMI

Siber alana ekosistem yaklaşımı; egemenlik temelli çözümlerin yetersiz olduğunu vurgulayan, siber alanın dinamik ve çok aktörlü yapısı ile teknolojik, sosyal, ekonomik ve çevresel etkilerine odaklanan ve nihayet buradaki bilgi ekosisteminin hukuku ve kurumlarını dönüştürme kapasitesini inceleyen interdisipliner bir literatür yoluyla geliştirilmektedir.⁷⁵ Bu bölümde, ekosistem yaklaşımının kapsamı aktarıldıktan sonra, AİHM içtihadında giderek farklı hak alanlarına doğru genişleyen iyi yönetim testi ile yatay etki kavramının ekosistem olarak siber alanda uygulanma kapasitesini sorgulayacağız. Bunun nedeni, ekosistem yaklaşımında, siber alandaki tüm aktörlerin siber alanın hukukunun oluşmasına katılımlarının ve sorumluluklarının öne çıkarılmasıdır.

⁷⁵ Siber suçların analizinde aktörlerin yarışmacı, yağmacı ya da işbirliğine dayanan eğilimlerini, siber alandaki endüstri, suç örgütleri ve güvenlik odaklı aktörlerin kapasite ve rasyonelitetlerini ele alan çalışma için Bkz. Benoît Dupont, 'The Ecology of Cybercrime' in Rutger Leukfeldt and Thomas J. Holt (eds), *The Human Factor of Cybercrime* (Routledge 2021) 389-400; Dijital teknolojiler aracılığıyla birbirine bağlanan bilgi ekosistemlerinin veri koruma, egemenlik ve dijital yönetimde yarattığı sorunlar ekseninde idare hukuku ve uluslararası hukukun dönüşümü inceleyen çalışma için Bkz. Cătălin-Silviu Savaru and Christina P. Tache, 'Knowledge Ecosystems in the Digital Age on Reshaping Administrative and International Law' (2024) (1)[2] *Journal of Knowledge Dynamics* 81-91.

Dijital ekosistem; dijital bilginin transferi için gerekli olan fiziksel altyapı sistemlerinin, elektronik ağların, çevrim içi ve çevrim dışı platformların, bunların her birinin işleyişini düzenleyen kuralların ve aktörlerin tamamını ifade eden bağlantılı sistem olarak tanımlanmaktadır.⁷⁶ Sistemlerin sistemi olarak adlandırılan siber alan ise bir mühendislik sistemi olmasından ziyade, üyelerinin rekabet etme ve uyumlanma kapasitesine göre hayatta kaldığı, kendi kendini düzenleyen ('self-regulating'), sürekli gelişen, interaktif bir ekosistemdir.⁷⁷ Tallinn Kılavuzunu hazırlayan uluslararası uzmanlar siber alanı; fiziksel, mantıksal, sosyal tabakalardan oluşan çok katmanlı bir yapı olarak tanımlamıştır. Fiziksel katmanda donanım ve kablolar, birden fazla ağı birbirine bağlayan *router*lar, sunucular ve bilgisayarlardan oluşan fiziksel ağlar yer almaktadır. Mantıksal katmanda, ağ araçları arasında bağlantı kuran uygulamalar, veriler ve veri değiş tokuşunu sağlayan protokoller yer almaktadır. Sosyal katmanda ise siber alanda faaliyet gösteren bireyler ya da gruplar yer almaktadır.⁷⁸ Tallinn Kılavuzundaki yaklaşım, çok katmanlılık ekseninde ekosistem yaklaşımını kısmen desteklese de egemenlik odaklı çözüm önerileri baskın gelmektedir. Buna göre; siber faaliyetler birçok egemen sınırdan, uluslararası sulardan, dış uzaydan ya da uluslararası hava sahasından geçerek gerçekleşse dahi, bu faaliyetleri gerçekleştiren kişi ya da yapılar bir ya da birden fazla devletin egemen yetki alanındadır. Ayrıca devletler, uluslararası insan hakları hukuku ya da teamül hukuku kurallarına uygun olarak topraklarında bulunan herhangi bir siber altyapının internet bağlantısını tamamen veya kısmen kesme hakkına da sahiptir.⁷⁹

Bununla birlikte siber alan yönetişi ('cyber governance') kavramı, ekosistem tartışmasının zeminini oluşturabilecek güçtedir. Mihr; siber yönetişi, düzenleyici ve usuli düzenek olarak tanımlamaktadır. İyi yönetişim ('good governance') ilkeleri ve insan hakları normlarına dayanan bu sistemde, iyi yönetişimin katılımcılık ve şeffaflık boyutları ile insan haklarının hesap verebilirlik amacı yönlendirici olacaktır.⁸⁰ Liaropoulos; yönetişimin 3 farklı model ekseninde hayata geçirilebileceğini belirtmiştir. Siber alan devlet odaklı küresel yönetim anlayışından farklı olduğundan; dağıtık ('distributed'), çok taraflı ('multilateralism') ve çok paydaşlı ('multi-stakeholderism') yönetim yaklaşımlarını içerisinde barındırır.⁸¹

⁷⁶ Ahreum Lee, 'Human Rights Actors in the Digital Information Ecosystem' (Report to the *Office of the High Commissioner for Human Rights* 2016) 7-8.

⁷⁷ Kari Lippert and Robert Cloutier, 'Cyberspace: A Digital Ecosystem' (2021) (9)[3] *Systems* 48.

⁷⁸ Tallinn Kılavuzu (n 15) 12.

⁷⁹ Tallinn Kılavuzu (n 15) Bölüm 6.

⁸⁰ Anja Mihr, *Cyber Justice Human Rights and Good Governance for the Internet* (Springer 2017) 71-79.

⁸¹ Liaropoulos (n 4) 25-35.



Dağıtık yönetim yaklaşımında, internetin devletlerin egemenlik sahasına indirgenemeyeceği mottosu ön plandadır. Dahası, siber alanın bir küresel müşterek ('global commons') olarak tanımlanması çabaları da dağıtık yönetime içkin bir tartışmadır. Al Asyari; siber alanın tüm insanlığı ilgilendiren bir işlevinin olması nedeniyle, askeri amaçlardan arındırılması ve barışçıl kullanımının kabul edilmesi gereğini savunmaktadır.⁸² Tsagourias; geçen yüzyılın küresel müşterek ya da *res communis*leri olarak tanımlanan açık deniz, Antarktika ve dış uzaya benzer şekilde, siber alanın da bu yüzyılın hukuki-politik -teknik inşası ('construct') müşterek olarak tanınmasının mümkün olduğunu; ancak bu tanınmanın dahi oto-limitasyon yoluyla devletlerin egemen iddialarından vazgeçmesi yoluyla yapılacağını hatırlatmaktadır.⁸³ Küresel müşterek tanımına karşı çıkan görüşler, siber alanda fiziksel mekân ve sınırların olmadığını; ancak veri ve bilgi transferini kolaylaştıran fiziksel altyapının var olduğunu, bu altyapı üzerinde küresel müştereklerden farklı olarak özel mülkiyetin söz konusu olabildiğini ve bunların da bir devletin egemenlik sahasında bulunduğunu ileri sürmektedir.⁸⁴ Mueller ve Xinmin ise siber alanı *sui generis* bir statüye yerleştirmektedir. Xinmin; siber alanı, gerçeklik ve virtüaliteyi birleştiren, egemenlik ve küresel müşterek niteliğini eş zamanlı barındıran yer olarak tanımlarken,⁸⁵ Mueller, mülkiyet ve müşterek özelliğinin eş zamanlı imkânına vurgu yapmaktadır.^{86, 87}

Çok taraflı yönetim; siber alan devletler tarafından düzenlenmediğinde bir tabii hal ortamı oluşacağı ve bunun da ulusal güvenlik sorununa neden olacağından hareket ederek, egemenlik eksenli düzenleme ve kontrol gereğini öne çıkarmaktadır. *Çok paydaşlı yönetim*de ise, Westphalia tipi egemenlik anlayışı korunmakla birlikte, siber alanda faaliyet gösteren devlet ve devlet dışı tüm aktörlerin (teknoloji şirketleri, arama motorları, internet kullanıcıları, sivil toplum vd.) siber alanın düzenlenmesine katıldığı ve sorumluluk aldığı bir çerçeve esastır. Bu yaklaşım BM Genel Kurulu'nun 57/239 sayılı kararında⁸⁸ benimsenen çok

⁸² Haekal Al Asyari, 'Cyberspace as a Common Heritage of Mankind: Governing Normative Limitations of the Internet by Virtue of International Law' (2023) (69) [4] *Auc Iuridica* 211-228.

⁸³ Tsagourias (n 54) 25-28.

⁸⁴ Liapopoulos (n 4) 28.

⁸⁵ Ma XinMin, 'Key Issues and Future Development of International Cyberspace Law' (2016) (2) [1] *China Quarterly of International Strategic Studies* 125.

⁸⁶ Mueller (n 39) 795.

⁸⁷ Verinin üretildiği, toplandığı, işlendiği ya da kullanıldığı veri ekosistemini müşterek olarak kabul etmeyi öneren görüş için Bkz. Nadezhda Purtova, 'Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons' in Samantha Adams, Nadezhda Purtova and Ronald Leenes (eds), *Under Observation: The Interplay Between eHealth and Surveillance* (Springer 2017) 177-210.

⁸⁸ Creation of a Global Culture of Cybersecurity (UNGA 2003) A/RES/57/239.

paydaşlı küresel bir siber güvenlik oluşturma hedefinden kaynağını almaktadır. Hedefi ise bir tür siber alan sosyal sözleşmesi oluşturmaktır.⁸⁹

Hukukun, siber alanın yukarıda ortaya konan ekosistemsel gereklerine ayak uydurması bütünüyle mümkün değildir. Dahası toplumsal yaşamı düzenleyen hukukun sosyal ve teknolojik gelişme hızını yakalamasını beklemek, istikrar ve hukuk güvenliği bakımından da sorunlar doğurabilecektir. Yapılması gereken gelişmeleri dikkatli izleyerek ihtiyaçları doğru tespit etmesi ve düzenlemesi olacaktır. Nitekim bu amaçla mevcut hukuki araçların siber alana uyarlanması ve/veya ihtiyaçlara yönelik yeni hukuki kurumlar yaratılması savlanmaktadır.

Siber alandaki çok paydaşlı yapının unsuru olan insan öznelerine yeni haklar tanınması ya da mevcut maddi ve usuli hakların siber alana uyarlanması ilk öneridir. 20. yüzyılın çevrimdışı ortamında yazılan sert veya yumuşak hukuk belgelerinin ürünü olan insan haklarının, çevrimiçi dünyaya ve siber alana uyarlanması, konvansiyonel egemenlik teorisinin siber alanda da geçerli olması yaklaşımıyla aynı temelden doğmaktadır. Burada, çevrimdışı ve çevrimiçi haklar arasında normatif eşdeğerlilik ('normative equivalency') olduğu tezleriyle, siber alanın işleyiş dinamiklerine uygun yeni haklar tanınması tezleri görülmektedir.⁹⁰ Normatif eşdeğerlilik bakımından, BM İnsan Hakları Komitesinin 2011 tarihli 34 Numaralı Genel Yorumu⁹¹ ile BM İnsan Hakları Konseyinin 2012 tarihli kararı yol göstericidir.⁹² Tallinn Kılavuzunun 35. Maddesi, uluslararası insan hakları sözleşmeleri ve teamül hukukunun siber faaliyetlere uygulanmasının mümkün olduğunu ifade etmiştir. Kılavuzda özel olarak anılan haklar düşünce ve ifade hürriyeti, özel yaşam/mahremiyet hakkı, adil yargılanma, barışçıl toplanma ve gösteri hürriyeti, özgürlük ve güvenlik hakkı, hakaret ve karalamadan korunma hakkıdır.⁹³ Bunlar yanında devletler de siber alanda korunması gereken hak kategorilerini tanımlayan kararlar almaktadır. Kılavuzda sayılan haklara ek olarak örneğin internete erişim, bilgi arama-alma ve yayma hakkı, eğitim hakkı, sağlık hakkı, vicdani kanaat hürriyeti, ayrımcılık yasağı ve şirketlerin tüm müşterilerin mahremiyet hakkını koruması, devletlerin tutum belgeleri ('position papers') yoluyla deklare edilebilmektedir.⁹⁴

⁸⁹ Liaropoulos (n 4) 29.

⁹⁰ Dafna Dror-Shpoliansky and Yuval Shany, 'It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights - A Proposed Typology' (2021) (32)[4] *European Journal of International Law* 1249–1282.

⁹¹ General Comment No.34 on Article 19: Freedoms of Opinion and Expression (UN Human Rights Committee 2011) 29/07/2011.

⁹² The Promotion, Protection and Enjoyment of Human Rights on the Internet (UN Human Rights Council 2012) A/HRC/32/L.20.

⁹³ Tallinn Kılavuzu (n 15) 187.

⁹⁴ Michael Schmitt and Liis Vihul, 'European Approaches to the Application of International Law in Cyberspace: A Comparative Legal Analysis' (2024) *EU Cyber Direct* 64–67.



Yeni haklar türetilmesi gereği savı ise soyut ve genel hak tanımlarının dijital alana uyarlanmasıdaki normatif ve pratik zorluklara, dava edilebilirlik bakımından ortaya çıkacak belirsizliklerin yaratacağı kısıntılara dayanmaktadır.⁹⁵ Her iki yaklaşımı harmanlayan bir çerçevede mevcut hakların *dijital habeas corpus*unun tespit edilmesi ve koşullar dahilinde yeni hakların türetilmesi de öneriler arasındadır.⁹⁶

Mevcut hakların uyarlanması ya da yeni haklar tanınması halinde, muhataplar bakımından da düzenleme gerekecektir. Devlet makamlarına ve devlet dışı aktörlere karşı ileri sürülebilecek, onları haklara saygı göstermeye zorlayacak teknolojik ve yatay bir hak arama ve adil yargılanma ('technological and horizontal due process') usulünün geliştirilmesi gereği önerisi⁹⁷ de siber alana ekosistemsel yaklaşımın parçasıdır.

AIHM'in birinci bölümde andığımız Centrum För Rättvisa/İsveç kararında (Para. 372-373) ve ardından Big Brother Watch ve Diğerleri/B.K. (B.D.) kararında (Para.425) kitlesel izlemenin Sözleşme düzenindeki yeri belirlenirken, izleme teknolojilerinin teknik gereklerini dikkate alan ve bunu insan hakları koruma sistemi içine yerleştiren bir hukuki-teknik terminoloji oluşturulmuştur. Bu doğrultuda, devletlerin ulusal güvenlik meşru amacını aşındıran keyfilik ve kötüye kullanım riskini engellemek ve 8. maddedeki hak ve özgürlüklerin etkili korunması için teknoloji alanında kullanılan uçtan uca şifrelemeye benzer şekilde, uçtan uca bir hukuki güvence sistemi ('end-to-end safeguards') kurulması, haklara müdahalede yasallık ve öngürülebilirlik bağlamında hukuk devletinin gereği ve devletin takdir yetkisinin sınırı olarak anılmıştır.⁹⁸

⁹⁵ Mart Susi, *The Non-coherence Theory of Digital Human Rights* (Cambridge University Press 2024) Özellikle Bkz. 'The Doctrine of the Sameness of Rights Online and Offline' ve 'Claims of New Internet-Specific Human Rights' Bölümleri.

⁹⁶ Oreste Pollicino, 'Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and its Possible Solutions' (EctHR 2022) <https://www.echr.coe.int/documents/d/echr/Intervention_20210415_Pollicino_Rule_of_Law_ENG> erişim tarihi: 14.02.2025.

⁹⁷ Pollicino (n 92).

⁹⁸ Avrupa Birliği Adalet Divanının yakın tarihli kararı, yorum yöntemleri (somut olayda teleolojik yorum) yoluyla mahkemelerin siber alana nüfuz etme kapasitesinin geleceği bakımından bir örnektir. Olayda, otomasyona bağlı kredi değerlendirmesinde olumsuz rapor verilen bir kişinin, Genel Veri Koruma Tüzüğü (GDPR) Madde 15/1/h kapsamındaki hakları somutlaştırılmıştır. Buna göre; otomasyona bağlı karar alma ve profillemeye kullanılan kodun mantığı, yürütülen sürecin usulü, amacı ve sonuçlarına dair ilgili, önemli ve anlaşılabilir bilgiye ('meaningful information') erişim bir haktır ve bu hak yargı yollarına başvuru ve diğer hakların etkili korumasında ön koşuldur. Bkz. ABAD, C-203/22- Dun & Bradstreet Austria, K.T. 27/02/2025.

1. İyi Yönetişim İlkesi Ve Siber Alandaki Aktörlerin Sorumluluğunun Dengelenmesi

İyi yönetim, kalkınma alanında 1989'da ortaya çıkan⁹⁹ ve zamanla yumuşak hukuk ('soft law') belgeleri¹⁰⁰ ve yargı kararları yoluyla hukuk alanına aktarılan bir kavram olarak, AİHM içtihadında, öncelikle mülkiyet hakkı kapsamında (P1-1) kamu gücü kullanan makamlar ile vatandaşların hak ve yükümlülüklerinin dengelenmesinde kullanılmıştır. Gelineen noktada iklim krizine karşı devletlerin pozitif edimlerinin kapsamının belirlenmesinde¹⁰¹ unsurlarına referans verilen veya uygulanacak hukuk ve/veya ölçülülük testinin bir unsuru olarak karşımıza çıkan bir ilkedir. İçtihadta istikrarlı bir uygulaması olmasa da, kavramın normatifleştirilmesi çabası^{102, 103, 104} somuttur.

AİHM'in iyi yönetim kavramını açıkça kullandığı ilk karar 2009 tarihli Moskal/Polonya kararıdır.¹⁰⁵ Moskal'daki ilkeler ise ilk kez Beyeler/İtalya kararında¹⁰⁶ şekillendirilecektir. Beyeler kararı; kamu gücü kullanan makamlar bakımından, yeni pozitif yükümlülükler öngörürken başvuruçular bakımından da, hakkın kötüye kullanılmasını oluşturmayacak ve özen yükümlülüğü gerektiren davranış sorumluluğu belirlenmiştir. Bu ilkeler, Moskal kararında açıkça zikredilecek olan iyi yönetim testinin unsurları olacaktır. Bunlar şu şekilde özetlenebilir:

- Kamu gücünün zamanında kullanılması ('*In Good Time Principle*' / '*Reagissement en temps utile*')
- Kamu gücünün tutarlılığı ('*Utmost Consistency Principle*' / '*Reagissement avec la plus grande cohérence*')
- Olaya uygun çözüm üreten idare ('*Appropriate Manner Principle*' / '*Reagissement de façon correcte*').¹⁰⁷

⁹⁹ Sub-Saharan Africa, From Crisis to Sustainable Growth (The World Bank (1989) <<https://documents1.worldbank.org/curated/en/498241468742846138/pdf/multi0page.pdf>> erişim tarihi:23.03.2025.

¹⁰⁰ Kavrama atfı yapan ilk yumuşak hukuk belgeleri için Bkz. Development and International Economic Cooperation: An Agenda for Development (UN General Assembly A/48/935, 06/05/1994)§118-138; Development Cooperation Policies (PACE Resolution 1060 (1995); United Nations Millennium Declaration (UN General Assembly, A/RES/55/2, 18/09/2000).

¹⁰¹ AİHM, Verein Klimaseniorinnen Schweiz ve Diğerleri/ İsviçre (B.D.), B. No. 53600/20, 09/04/2024, §548, 573.

¹⁰² AİHM, Gürcistan/Rusya (II) (B.D.), B.No.38263/08, K.T.21/01/2021, Yargıç Dedov, § 6.

¹⁰³ AİHM, Ahmet Yavuz Yılmaz/Türkiye, B.No.48593/07, K.T.10/11/2020, Yargıç Kuris ve Pavli karşı oy yazısı, §5.

¹⁰⁴ AİHM, Cano Mayo/İspanya, B.No. 3142/11, K.T.11/10/2016, Yargıç Dedov Karşı oy yazısı, §2.

¹⁰⁵ AİHM, Moskal/Polonya, B.No. 10373/05, 15/09/2009, §72.

¹⁰⁶ AİHM, Beyeler/İtalya, B.No. 33202/96, K.T. 05/01/2000, §120.

¹⁰⁷ Agne Andrijauskaitė, 'Good Governance in the Case Law of the ECtHR: A (Patch)Work in Progress' (2018) *Presented Paper in ICON-S Conference: Identity, Security, Democracy: Challenges for Public Law, Hong Kong*.

Moskal kararında, bu ilkelere idari makamların azami titizlik göstermeleri ('utmost scrupulousness') yükümlülüğü eklenmiştir.

İyi yönetim; siber alan ekosisteminde, devletler bakımından hakların korunmasında zamanlama, duruma uygun çözüm üretme ve tutarlılık bakımından bir test yapılmasına imkân sağlayabilecektir. Özellikle siber alanda hak ihlallerinin önlenmesi amacıyla, uçtan uca güvenceler içeren mevzuat oluşturulması, siber güvenlik önlemlerinin alınması, altyapının kurulması gibi idari kapasitenin geliştirilmesi ve hak ihlallerine karşı etkili başvuru yollarının ihdası, maddi ve usuli pozitif yükümlülükler kapsamında söz konusu olabilecektir. Dahası Big Brother Watch ve Diğerleri/B.K (B.D.) kararında bazı yargıçlar; kitlesel izleme pratikleri sürekli bir kişisel-işsel kontrolü dayattığı için bireylerin özgürlük algısının ve nihayet demokratik özerk yönetişimin ('democratic self-governance') zarar göreceğini vurguladığından,¹⁰⁸ siber alan ekosisteminin hukukuna bütüncül yaklaşılmalıdır.

Öte yandan iyi yönetim testi; hak öznelerinin iyi niyetli olup olmadıklarını, kamu gücü kullanan makamlar ile kişilerin tutumlarının dengelenmesini ve kişilere yüklenen külfetin ölçülülüğünün değerlendirilmesini de içermektedir. Bu değerlendirmede, karşı-kamusallık bölümünde vurgulanan kırılganlık testinin devreye sokulması, iyi yönetim testinde çıkarlar arasında adil bir dengenin kurulması bakımından da önem arz edecektir. Örneğin Le Marrec kararında,¹⁰⁹ Fransa sosyal yardım ödenekleri sistemine (CAF) online giriş yapan başvuru- nın bilgisayarının IP (internet protokolü) adresinin, siteyi barındıran sunucu tara- fından 'diğer ülke' coğrafi işaretiyle değiştirilmesiyle başlayan ve başvuru- cunun sosyal yardım hakkını kaybettiği bir şikayet incelenmiştir. CAF; IP adresindeki bu değişiklikten yola çıkarak, başvuru- cunun Fransa'da ikamet edip etmediğini inceleme altına aldığı- nda, birçok gelir beyanının yapılmadığını tespit etmiştir. Başvuru- cu, Fransa'da bulunduğunu ve sadece VPN (sanal özel ağ) kullandığını beyan etse de, iyi niyetli olmadığına kanaat getirilerek yardım hakkı kaybettiril- miştir. Mahkeme yaptığı değerlendirmede; IP adresinin bir meta veri olduğunu ve başvuru- cuya dair özel kişisel verilere erişim sağlamadığını, başvuru- cunun IP adresinin CAF yetkilileri tarafından görülmeyeceğine dair bir beklentisinin makul olarak bulunamayacağını, veri kullanımının minimizasyonu ilkesine uygun olarak hareket edildiğini vurgulamıştır. Ulusal makamların sosyal yardım yolsuzlukla- rını engellemede meşru bir yararının olduğunu belirten Mahkeme, yaptırım ağır olsa da, 8. Madde kapsamındaki başvuru- nun iyi temellendirilmediğine ve haliyle maddenin ihlal edilmediğine hükmetmiştir.

Siber iyi yönetim konusunda son sorun, bu alanın hukukunun gelişmekte olması ve bu alanın hukuki boşluklar barındırmasıdır. Bu da kamu idareleri ile

¹⁰⁸ (n 47) Bkz. Yargıçlar Lemmens, Vehabović ve Bošnjak'ın ayrık görüşü, § 2-9.

¹⁰⁹ AİHM, Le Marrec/Fransa, B. No. 52319/22, K.T.05/11/2024, § 77-83.

kişilerin tutumlarının dengelenmesinde devletler lehine sonuç doğurabilmektedir. Örneğin, Paul Getty ve Diğerleri/İtalya kararında AİHM; kültür varlıklarının iadesine dair ilgili dönemde uluslararası bağlayıcı kurallar olmaması nedeniyle, İtalyan makamlarının ihmali ve tutarsız davranışlarını (başlatılan soruşturmanın devam ettirilmemesi) başvuruçuların tutumu ile dengelemiş ve nihayetinde başvuruçuyu iyi niyetli kabul edilse dahi mülkiyet hakkının ihlal edilmediğine hükmetmiştir.¹¹⁰ Uyuşmazlık doğrudan konumuzla ilgili olmasa da siber alan hukukundaki boşluklar, iyi yönetim testiindeki adil denge ve aşırı külfet incelemesi bakımından etki doğurabilecek güçtedir.

2. Yatay Etki Ekseninde Gerçek Kişiler İle Platformların Hak Ve Sorumlulukları

Siber alanda faaliyet gösteren özel kişiler arasında büyük teknoloji şirketleri ya da platformlar olabildiği gibi açık ya da anonim kimlikli gerçek kişiler de özgürlük ve sorumluluk ekseninde sözleşmesel standartlara tabi tutulmaktadır. Yatay etki; temel hakların bilişim ve teknoloji çağında etkili korunması,¹¹¹ hak ve özgürlüklerin yalnızca devlet organlarına karşı değil; sosyal alana ilişkin hükümler yoluyla kişilere de benimsenmesi¹¹² işlevini görmektedir.

AİHM; AİHS'in 1., 13., 17., maddeleri ile diğer maddelerde yer alan meşru sınırlama nedenleri ekseninde özel kişilerin insan hakları alanındaki sorumluluklarını gerekçelendirmektedir. Özel kişilerin neden olduğu hak ihlallerine karşı etkili başvuru yollarının yokluğu, ileri sürüldüğü hakla birlikte Sözleşmenin 13. maddesinin ihlalini de getirebilmektedir. Özellikle Sözleşmeye dayalı ilişkilerde dahi taraflar arasındaki güç dengesi ve hiyerarşi olup olmadığı, özel kişilerin işlemlerinin yargısal denetimin sınırını dikkate alarak Mahkeme, yatay etkiye dair bir karara varmaktadır.¹¹³

Siber alanda yatay etkinin uygulaması bakımından aşağıda ikili bir değerlendirme yöntemi benimsedik. İçtihatla özellikle ifade hürriyeti bakımından; platformlar, kullanıcılar ve daha genel toplumun çıkarları arasında bir denge kurulmaya çalışılırken, ulusal makamların negatif ve pozitif yükümlülüklerinin kapsamı da şekillenmektedir.

a. Gerçek Kişiler Bakımından

Mahkeme; sosyal medya platformları ya da blog sayfalarında paylaşılan ya da üretilen içerik nedeniyle iç hukukta yaptırıma uğrayan kişilerin başvurularında;

¹¹⁰ AİHM, The J. Paul Getty Trust ve Diğerleri/İtalya, B. No. 35271/19, 02/05/2024, § 400.

¹¹¹ Korkut Kanadoğlu, 'Alman Anayasa Hukuku Öğreti Ve Uygulamasında Temel Hakların Yatay Etkisi (Üçüncü Taraf Etkisi)' (2024) (41)[1] *Anayasa Yargısı* 596-597.

¹¹² Oya Boyar, *Anayasa ve Özel Hukuk* (On İki Levha 2019)19.

¹¹³ Bu standartların uygulandığı karar için Bkz. AİHM, Semenya/İsviçre (B.D.), B. No. 10934/21, K.T.10/07/2025.



kişilerin meslekleri, yaydıkları bilginin doğruluğu ve niteliği, bilginin yayılma hızı ve takipçi kitlesinin büyüklüğü ile yaptırımın caydırıcı etkisi bakımından değerlendirme yaparak sonuca ulaşmaktadır.

Örneğin Melike/Türkiye kararında¹¹⁴ Mahkeme; Milli Eğitim Bakanlığında sözleşmeli personel statüsünde çalışan kişinin, Facebook platformundaki beğenileri ('like') ve iki yorumu nedeniyle, sözleşmesinin İş Kanununun 25. maddesi doğrultusunda, ahlak ve iyi niyet kurallarına uymayan davranışlar kapsamında tazminatsız feshedilmesi yaptırımını 10. madde bağlamında incelemiştir. Mahkeme, kişinin kamu görevlisi statüsünde olmaması nedeniyle kendisinden beklenen sadakat ve bağlılığın kamu görevlileri ile aynı olamayacağını; başvuranın kıdemi ve yaşı yanında beğenilerinin içeriğinin, çalışma barışını bozup bozmadığının ve iş ilişkisine etkisinin ulusal makamlar tarafından değerlendirilmemesinin yaptırımı ölçüsüz kıldığına hükmetmiştir.¹¹⁵ Öte yandan holistik tıp üzerine web sayfasında, doğada hastalık olmadığı ve aşılardan hiçbir zaman hastalıkları iyileştirmedigine dair paylaşımlar yapan bir tıp doktorunun, Tabip Odası tarafından disiplin cezasına tabi tutulması olayında; doktorun mesleki sorumluluğu, kamu sağlığının korunması ve içeriğin bilimsel bilgiye aykırı olması karşısında ifade özgürlüğüne yapılan müdahalenin ölçülü olduğuna kanaat getirmiştir.¹¹⁶ Ancak güzellik salonu işleten bir kişinin nispeten az takipçili Instagram hesabında, yaşadığı bölgede COVID-19 olmadığına dair içerikler paylaşması sonucunda, yanlış bilgi yayma ('disseminating untrue information') gerekçesiyle 390 Euro para cezası alması, 10. Maddenin ihlalini getirmiştir.¹¹⁷ Karara mutabık görüş yazan hakimler ayrıca, dezenformasyonla mücadele gerekçesiyle ulusal makamlarca doğru veya yanlış bilgi tasniflerinin ve bunlar üzerinden yaptırımların dijital dünyada ifade hürriyeti üzerindeki olası sansür etkisine dikkat çekmiştir.

Savva Terentyev/Rusya kararında,¹¹⁸ seçim döneminde muhalefet adaylarına destek verdiği bilinen bir gazetede polis tarafından yapılan arama sonrasında, bazı blog sayfalarında yayımlanan açıklamalar ve bunlara yapılan yorumlarda polisler karşı kullanılan ifadeler nedeniyle kişilere ceza verilmiştir. Mahkeme, kullanılan ifadelerin aşağılayıcı, saldırgan ve düşmanca olduklarını kabul etse de, ifadelerin muhatabı polislerin özel olarak korunması gereken bir grup olmadığına, açıklamaların yayımlandığı blog sayfasının takipçi kitlesinin ve başvuru-

¹¹⁴ AİHM, Melike/Türkiye, B.No. 35786/19, K.T.15/06/2021, § 50-51.

¹¹⁵ Ülke gündemi, siyasi gelişmeler ve hukuki meseleler üzerine Facebook sayfasında paylaşımlar yapan bir yargıcın paylaşımlarının üçüncü kişiler ve haber portalları yoluyla yayılması ve bir paylaşımında bir savcıya dair haber bağlantısı ('hyperlink') vermesi nedeniyle maaştan kesme cezası alması, ifade hürriyetinin ihlalini getirmiştir. Bkz. AİHM, Danilet/Romanya, B. No. 16915/21, K.T. 20/02/2024.

¹¹⁶ AİHM, Bielau/Avusturya, B. No. 20007/22, K.T.27/08/2024.

¹¹⁷ AİHM, Avagyan/Rusya, B. No. 36911/20, K.T. 29/04/2025.

¹¹⁸ AİHM, Savva Terentyev/Rusya, B. No. 10692/09, K.T.28/08/2018, § 76-84

cunun yorumlarının etkisinin ölçülmediğini vurgulayarak 10. Maddenin ihlaline hükmetmiştir.

Alexandru Pătraşcu/Romanya kararı,¹¹⁹ bir *blogger*ın üçüncü kişilerin yorumlarından sorumlu tutulması nedeniyle ifade hürriyetinin ihlal edildiğine dair bir şikayete ilişkindir. Olayda, ulusal operadaki yabancı müzisyenlerin işten çıkarılması talepleri ile yabancı düşmanlığını kapsayan bir dizi konu, yaklaşık 3 ay boyunca yazı ve yorumlar yoluyla blogta işlenmiştir. İç hukuk sürecinin sonunda, başvuru hem kendisinin hem de sayfalarında yorum yapan üçüncü kişilerin beyanlarından sorumlu tutulmuş ve tazminat ödemeye mahkum edilmiştir. AİHM, başvuru blog sayfasının ödüllü ve bilinebilir bir mecra olduğunu dikkate almıştır. Ancak bu mecranın, ulusal yargı makamları tarafından bir televizyon sunucusu ya da platforma benzer içerik sağlayıcı olarak değerlendirilmesini yasalık bakımından sorunlu bulmuştur.

Sanchez/Fransa başvurusunda¹²⁰ ise milletvekilliğine aday bir belediye başkanının Facebook sayfasında, üçüncü kişilerce yapılan ırkçı ve yabancı düşmanı yorumlar karşısındaki tutumu iç hukukta para cezası ile sonuçlanmıştır. Mahkeme; içeriklerin yayımlanmadan önceki denetimi noktasında platformun ve hesap sahibi kişinin sorumluluğunu ayıran bir yaklaşım benimsemiştir. Başvurucunun siyasetçi kişiliği, olayın seçim döneminde gerçekleşmesi, para cezasıyla sınırlı cezalandırmanın kişinin kariyeri üzerinde ölçsüz etkisinin olmaması gerekçeleriyle, ifade hürriyetine yapılan müdahaleyi ölçülü bulmuştur. Karşı oylar öte yandan, başvuru 'içerik üreticisi' olarak kabulünün ve buradan kaynaklı sorumluluğun iç hukukta öngörülebilir olmadığına dayanarak çoğunluk görüşünü eleştirmiştir.

b. Platformlar Bakımından

AİHM; yazılı basın-internet medyası ayrımı, sosyal medya platformları ve haber portalları farkı ve nihayet bunların büyüklükleri ve içerik üretme-yayımlama durumuna göre sorumluluğun kapsamını belirlemektedir.¹²¹ 2011 tarihli Editorial Board of Pravoye Delo ve Shtetel/Ukrayna kararı¹²² Mahkeme ilk kez internet medyası ile yazılı basın arasında düzenleme, denetim ve yükümlülükler bakımından karşılaştırma yapmıştır. Buna göre ilkinin yayılma hızı, olumlu etkisi ya da verebileceği zarar diğerinden daha fazla iken düzenlenmesi ve denetimi, bilgi iletişim teknolojilerinin özel durumu nedeniyle daha zayıftır. Bu nedenle, devletlerin bu alandaki içerikleri düzenleme politikalarının, hak ve hürriyetlerin

¹¹⁹ AİHM, Alexandru Pătraşcu/Romanya, B.No. 1847/21, K.T.07/01/2025, §126-136.

¹²⁰ AİHM, Sanchez/Fransa (B.D.), B. No. 45581/15, K.T.15/05/2023.

¹²¹ İnternet hukukuna dair AİHM kararlarının daha detaylı incelemesi için Bkz. Mehmet Bedii Kaya, *İnternet Hukuku* (On İki Levha 2021, 2. Baskı) 207-485.

¹²² AİHM, Editorial Board of Pravoye Delo ve Shtetel/Ukrayna, B. No. 33014/05, K.T. 05/05/2011, §63-64.



etkili korunması için teknolojinin gereklerine uyarlanması gerekmektedir. Bu karar ile başlayan, Delfi As/Estonya¹²³ ile Atv Zrt/Macaristan¹²⁴ kararları ile çerçevesi kurulan içtihadta, geniş kitlelere hitap eden haber portallarının hem kendi yayınları hem de kullanıcılarca oluşturulan içeriklere dair özen yükümlülüğü kabul edilmiştir.

2015 tarihli Delfi As kararında ilk kez, kullanıcıların yorumları nedeniyle bir haber portalının tazminata mahkum edilmesi incelenmiştir. Estonya'nın en büyük internet haber portalı olan Delfi As, sınırlı sorumlu bir kamu taşıma şirketinin, donmuş deniz üzerindeki kamuya ait yollara ('ice road') zarar verdiği haberini yapmıştır. Bu haberin ardından anonim veya açık kimlikli kullanıcıların yaptığı yorumlarda, şirket yöneticilerine yönelik şiddet tehdidi dahil hakaretamiz ifadeler kullanılmıştır. Şirketin hissedarı bir kişi, siteye başvurmuş ve ifadeler kaldırılmıştır. Ancak şirketin tazminat istemi üzerine, haber portalı tazminat ödemeye mahkum edilmiştir. AİHM; kullanıcı yorumlarına dair rehber ilkeler oluşturan, nefret söylemi ve şiddet içerikli yorumlar için filtreleme sistemi kullanan ve şirket hissedarının şikayeti üzerine derhal kullanıcı yorumlarını kaldıran başvurusunun iyi niyetli hareket ettiğini kabul etmiş; ancak ödediği 320 Euro manevi tazminatı ölçülü bulmuştur. Bu sonuca varırken, ülkede en geniş platform olmaya devam etmesi ve iş modelini ('business model') değiştirmek zorunda kalmaması vurgusu karşı oylerde eleştirilmiştir. Online yayıncıların basın yerine girişimci olarak değerlendirilmesi ve takdir yetkisinin geniş olduğu ekonomik alan vurgusu yoluyla basın ve ifade hürriyetlerinin istisnaya uğratılması, bir nevi sansür olarak değerlendirilmiştir.

Atv Zrt başvurusunda, Jobbik isimli siyasi partinin bir milletvekilinin mecliste Yahudilerle ilgili yaptığı konuşma sonrası, 'parlamento aşırı sağ' etiketi ile Atv Zrt platformu tarafından haber yapılması nedeniyle platforma verilen cezadan şikayet edilmiştir. Ulusal makamların iddiası, bu etiketlendirmenin bir olgu aktarımı değil; özel görüş olduğu yönündedir ve platform tarafsız ve sorumlu gazeteciliğin gereği olan özen yükümlülüğünü yerine getirmemiştir. Başvurucu platform ise toplumdaki yaygın kanı¹²⁵ ve Meclis'teki söylevlere dayalı bir siyasi duruş tasnifi yaptığını belirtmektedir. Mahkeme; ulusal yargı makamlarının Jobbik partisinin siyasi ideolojisi noktasında net bir tespitinin olmaması nedeniyle, başvuru şirketin bu temelde bir müdahaleyi öngöremeyeceğini belirtmiş ve ihlal kararı vermiştir. Mesić/Hırvatistan kararında¹²⁶ ise bir internet haber portalının eski devlet başkanının görev sırasında yolsuzluk yaptığına dair belge yayınlaması

¹²³ AİHM, Delfi As/Estonya (B.D), B. No. 64569/09, K.T.16/06/2015, § 160-161.

¹²⁴ AİHM, Atv Zrt/Macaristan, B. No. 61178/14, K.T.28/04/2020, § 44-52.

¹²⁵ Jobbik partisinin ırkçı gruplar ile bağına dair bir videoya haber bağlantısı verilmesi ('hyperlinking') gerekçesiyle objektif sorumluluğun kabulünün caydırıcı etki sayılmasına dair Bkz. AİHM, Magyar Jeti Zrt/Macaristan, B. No. 11257/16, K.T.04/12/2018, § 69-83.

¹²⁶ AİHM, Mesić/Hırvatistan (No 2), B. No. 45066/17, 30/05/2023, § 80.

üzerine gelişen olaylar söz konusudur. Devlet başkanının tazminat taleplerinin iç hukukta reddi, AİHM bakımından ölçülü bulunmuştur. Kararın önemli kısmı ise haber platformlarının kullandığı dile dair beklenen özen yükümlülüğünün, bir mahkemenin cezai bir suçlamayı sağlam temellere dayandırmasında aranan titizlikle aynı olmadığına dair tespittir. Ancak karşı oylarda, platformların ifade hürriyeti karşısında kişisel özgürlüklerin daha az koruma gördüğüne dair bir eleştiri de söz konusudur.

Son olarak Podchasov/Rusya başvurusu;¹²⁷ terör bağlantılı faaliyetlerinden şüphelenilen 6 kişinin 12 Temmuz 2017'den itibaren yaptıkları görüşmeleri çözümlmek üzere Federal Güvenlik Servisince Telegram şirketinden teknik bilgi talep edilmesi ile ilgilidir. Telegram; bu emrin teknik olarak uygulanmasının mümkün olmadığını, zira başvuruçuların gizli sohbet modunda iletişim kurduklarını, bunun da uçtan uca şifrelendiğini iletmiştir. Bir arka kapı ('backdoor') yaratılarak özel iletişim kayıtlarına erişmenin ise sadece başvuruçular bakımından değil; tüm kullanıcılar ve dahi platformun kendisi için olumsuz sonuçlar yaratacağını söylemiştir. Mahkeme'ye göre, Rusya makamlarının sosyal ağ sağlayıcı Telegram'dan talebi, belirli kişilerin iletişim verisinin depolanması ve bu verinin 3. kişilerin erişimine açılması ile sınırlı değildir ve talep bir tür gizli izleme teşkil edebilecektir. Tüm iletişim bilgilerine erişime izin veren ve yeterli güvence içermeyen mevzuat, 8. Maddedeki hakkın özüne zarar verecektir.

SONUÇ

Bu çalışma kapsamında, siber kamusal alanı egemenlik, karşı-kamusallık ve ekosistem yaklaşımları ekseninde bir incelemeye tabi tutmaya çalıştık. Bu doğrultuda, siber alanın düzenlenmesi eğiliminin AİHM içtihadına yansıdığını; bu yansımanın egemenlik teorisi, insan haklarının korunması ve siber alanın aktörlerinin sorumluluğu bakımından somut olduğunu söylemek mümkündür. Siber egemenlik tesisine yönelik düzenleme ve uygulamalar, devletlerin ve Mahkemenin yargı yetkisinin kapsamının yeniden şekilleneceğine dair işaretler barındırmaktadır. Bununla birlikte bu şekillenmede hukuk yanında teknolojik, ekonomik, politik süreçlerin etkisi de yoğun bir biçimde gözlenecektir. Mahkemenin kullandığı terminolojiye de yansıyan bu etki, uluslararası hukukun temel aktörü olmaya devam eden devletlerin insan hakları alanındaki sorumluluklarının kapsamını da şekillendirecektir. Siber alanın karşı-kamusallık alanı niteliği; siber alanda görünürlüğü düzenleyen devlet ve devlet dışı aktörlerin yaklaşımları ile öznelerin dijital kırılganlığı ekseninde gelişmektedir. Ekosistem olarak siber alan yaklaşımın ise siber kapsayıcılık ve katılımcılık yerine yeni hiyerarşiler ve hak özneleri bakımından yeni sorumluluklar yaratabilecek dinamiklere yanıt verecek içerikte geliştirilmesi gerekecektir.

¹²⁷ AİHM, Podchasov/Rusya, B.No. 33696/19, K.T.13/02/2024, §66-81.

KAYNAKÇA

- Ackerman B, *We The People: Foundations* (Harvard University Press 1991)
- Akkuş B, ‘Devletin Etkin Kontrolünün Bulunmadığı Siber Alanda İnsan Hakları Yükümlülükleri Nelerdir?’ (2024) (6)[1] Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi 159-214
- Al Asyari H, ‘Cyberspace as a Common Heritage of Mankind: Governing Normative Limitations of the Internet by Virtue of International Law’ (2023) (69) [4] *Auc Iuridica* 211-228
- Amaritei I, ‘Les élections présidentielles en Roumanie : la Constitution contre Tik-tok’ (2024) *Questions Constitutionnelles: Revue de droit constitutionnel*
- Andrijauskaitė A, ‘Good Governance in the Case Law of the ECtHR: A (Patch) Work in Progress’ (2018) *Presented Paper in ICON-S Conference: Identity, Security, Democracy: Challenges for Public Law, Hong Kong*
- Arsava F A., ‘AİHK’nun Extraterritorial Geçerliliği Bağlamında AİHM’nin İçtihatlarında Görülen Hareketlilik’ (2019) (25)[2] *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 590-601
- Austin L M., ‘Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)’ in Austin Sarat (ed), *A World without Privacy: What Law Can and Should Do?* (Cambridge University Press 2014) 131-189
- Barlow J P, ‘A Declaration of the Independence of Cyberspace’ (1996) <<https://www.eff.org/cyberspace-independence>> erişim tarihi: 11.02.2025
- Berman P S., ‘Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to ‘Private’ Regulation” (2000) (71) *University of Colorado Law Review* 1263-1310
- Besson S, ‘The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to’ (2012) (25)[4] *Leiden Journal of International Law* 857-884
- Bignami F and Resta G, ‘Extraterritoriality’ in Giovanni De Gregorio, Oreste Pollicino, and Peggy Valcke (eds), *The Oxford Handbook of Digital Constitutionalism* (online edn, Oxford Academic 2024)
- Boyar O, *Anayasa ve Özel Hukuk* (On İki Levha 2019)
- Castells M, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press 2001) 247-275.
- Celeste E, ‘Digital Constitutionalism: A New Systematic Theorisation’ (2019) 33[1] *International Review of Law, Computers & Technology* 76-99
- Creation of a Global Culture of Cybersecurity (UNGA 2003) A/RES/57/239.

Çalı B, ‘Has ‘Control over Rights Doctrine’ for Extra-territorial Jurisdiction Come of Age? Karlsruhe, too, has Spoken, Now It’s Strasbourg’s Turn’ (EjilTalk 2020) <<https://www.ejiltalk.org/has-control-over-rights-doctrine-for-extra-territorial-jurisdiction-come-of-age-karlsruhe-too-has-spoken-now-its-strasbourgs-turn/>> erişim tarihi: 11.04.2025

Declaration on a Common Understanding of International Law in Cyberspace (Council of European Union, 18 November 2024) <<https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/>> erişim tarihi: 14.02.2025

Developments in the Field of Information and Telecommunications in the Context of International Security (UN General Assembly Resolution 31 December 2020) <<https://digitallibrary.un.org/record/3896180?ln=en>> erişim tarihi: 12.02.2025

Dror-Shpoliansky D and Shany Y, ‘It’s the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights - A Proposed Typology’ (2021) (32)[4] *European Journal of International Law* 1249–1282

Dupont B, ‘The Ecology of Cybercrime’ in Rutger Leukfeldt and Thomas J. Holt (eds), *The Human Factor of Cybercrime* (Routledge 2021) 389-400

Dzehtsiarou K, *Can the European Court of Human Rights Shape European Public Order?* (Cambridge University Press 2022)

Efrony D and Shany Y, ‘A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice’ (2018) 112 [4] *American Journal of International Law* 583–657

Fineman M A., ‘The Vulnerable Subject: Anchoring Equality in the Human Condition’ (2016) (20)[1] *Yale Journal of Law and Feminism* 8-14

Foucault M, ‘Des espaces autres Hétérotopies’ (1967) <https://historiacultural.mpbnet.com.br/pos-modernismo/Des_espaces_autres.pdf> erişim tarihi: 15.03.2025

Foucault M, *Dits et Ecrits* (Gallimard, 1994)

Fraser N, ‘Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy’ (1990) (12) [25/26] *Social Text* 56-80

General Comment No.34 on Article 19: Freedoms of Opinion and Expression (UN Human Rights Committee 2011) 29/07/2011

Gibson W, *Neuromancer* (Ace Book (Ebook 1984)

Gu H, ‘Data, Big Tech, and the New Concept of Sovereignty’ (2023) (29) *Journal of Chinese Political Sciences* 596-612



Habermas J, ‘The Public Sphere: An Encyclopedia Article’ Çev. Sara Lennox, and Frank Lennox (1974) (3) *New German Critique* 49-55

Hartzog W and Richards N M., ‘Privacy’s Constitutional Moment and the Limits of Data Protection’, (21) *Boston College Law Review* 1687- 1761

Hatipoğlu Aydın D, *Siber Alan ve Hukuk* (On İki Levha 2022)

Heri C, *Responsive Human Rights: Vulnerability, Ill-treatment and the EctHR* (Hart Publishing 2021)

Hertz N, ‘Neurorights – Do We Need New Human Rights? A Reconsideration of the Right to Freedom of Thought’ (2023) (16) [5] *Neuroethics*

International Law Commission’s Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA 2001) <https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf> erişim tarihi: 22.01.2025

Işık A, *İnternet Aktörleri ve Egemenliğin Değişen Boyutları: Digital Services Act ve Türk Mevzuatı Özelinde Bir İnceleme* (On İki Levha 2025, 2.Baskı)

Kaminski M E., ‘Binary Governance: Lessons from the GDPR’s Approach to Algorithmic Accountability’ (2019) (92) *California Law Review* 1554

Kanadoğlu K, ‘Alman Anayasa Hukuku Öğreti Ve Uygulamasında Temel Hakların Yatay Etkisi (Üçüncü Taraf Etkisi)’ (2024) (41)[1] *Anayasa Yargısı* 596-597

Kaya M. B, *İnternet Hukuku* (On İki Levha 2021, 2. Baskı)

Kempf V and Seignani S, ‘Capitalism and contested publicity. A conversation with Nancy Fraser’ (2023) (50)[1] *Philosophy & Social Criticism* 66-79

Koulos T, ‘A digital territory to be appropriated: the state and the nationalization of cyberspace’ (2022) *Open Research Europe*

Lee A, ‘Human Rights Actors in the Digital Information Ecosystem’ (Report to the *Office of the High Commissioner for Human Rights* 2016) 7-8

Lessig L, ‘The Laws of Cyberspace’, <https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf> erişim tarihi: 25.03.2025

Lessig L, *Code Version 2.0* (Penguin 2006)

Liaropoulos A N., ‘Cyberspace Governance and State Sovereignty’ in George C. Bitros and Nicholas C. Kyriazis (eds), *Democracy and an Open-Economy World Order* (Springer 2017) 25-35



- Lippert K and Cloutier R, 'Cyberspace: A Digital Ecosystem' (2021) (9)[3] *Systems*
- Mauri D, 'On American Drone Strikes and (Possible) European Responsibilities: Facing the Issue of Jurisdiction for 'Complicity' in Extraterritorial Targeted Killings' (2019) (28) [1] *The Italian Yearbook of International Law*, 249-272
- Mihr A *Cyber Justice Human Rights and Good Governance for the Internet* (Springer 2017)71-79
- Milanovic M, 'Jurisdiction, Attribution and Responsibility in Jaloud' (Ejil-Talk 2014) <<https://www.ejiltalk.org/jurisdiction-attribution-and-responsibility-in-jaloud/>>erişim tarihi:23.03.2025
- Mueller M, 'Against Sovereignty in Cyberspace' (2020) (22)[4] *International Studies Review*
- Pollicino O, 'Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and its Possible Solutions' (EctHR 2022) <https://www.echr.coe.int/documents/d/echr/Intervention_20210415_Pollicino_Rule_of_Law_ENG> erişim tarihi: 14.02.2025
- Purtova N, 'Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons' in Samantha Adams, Nadezhda Purtova and Ronald Leenes (eds), *Under Observation: The Interplay Between eHealth and Surveillance* (Springer 2017) 177-210
- Ryngaert C, 'Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts' (2023) (24)[3] *German Law Journal* 537-550
- Saracco R, 'Digital Twins: Bridging Physical Space and Cyberspace' (2019) 52 [12] *Computer* 58-64
- Savaru C S and Tache C P. T, 'Knowledge Ecosystems in the Digital Age on Reshaping Administrative and International Law' (2024) (1)[2] *Journal of Knowledge Dynamics* 81-91
- Schmitt M and Vihul L, 'European Approaches to the Application of International Law in Cyberspace: A Comparative Legal Analysis' (2024) *EU Cyber Direct* 64-67
- Schmitt M N. and Watts, S, 'Beyond State-Centrism: International Law and Non-state Actors in Cyberspace' (2016) (21)[2] *Journal of Conflict & Security Law* 600-606
- Schmitt M N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)

Susi M, *The Non-coherence Theory of Digital Human Rights* (Cambridge University Press 2024)

Takada T, Nakazato J, Orsholits A, Tsukada M, Ochiai H, and Esaki H, ‘Design of Digital Twin Architecture for 3D Audio Representation in AR’ (2024) *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications* 222-230

Taylor L, Floridi L, and Van der Sloot B, (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017)

The Promotion, Protection and Enjoyment of Human Rights on the Internet (UN Human Rights Council 2012) A/HRC/32/L.20

Tsagourias N, ‘The Legal Status of Cyberspace’ in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Elgar Online 2021)

Viljoen S, ‘A Relational Theory of Data Governance’ (2021) (131)[2] *Yale Law Journal* 623-634

XinMin M, ‘Key Issues and Future Development of International Cyberspace Law’ (2016) (2)[1] *China Quarterly of International Strategic Studies*

Yükselbaba Ü, ‘Kamusal Alan Modelleri ve Bu Modellerin Bağlıları’ (2011) (66)[2] *Journal of Istanbul University Law Faculty* 227-271

Kararlar

ABAD, C-203/22- Dun & Bradstreet Austria, K.T. 27/02/2025

AİHM, A.A ve Diğerleri /Kuzey Makedonya, B.No. 55798/16, K.T. 05/04/2022

AİHM, A.L. ve E.J./Fransa, B. No. 44715/20, K.T. 24/09/2024

AİHM, Ahmet Yavuz Yılmaz/Türkiye, B.No.48593/07, K.T.10/11/2020

AİHM, Alexandru Pătraşcu/Romanya, B.No. 1847/21, K.T.07/01/2025

AİHM, Al-Skeini ve Diğerleri/ Birleşik Krallık (B.D.), B. No.55721/07, K.T. 07/07/2011

AİHM, Atv Zrt/Macaristan, B. No. 61178/14, K.T.28/04/2020

AİHM, Avagyan/Rusya, B. No. 36911/20, K.T. 29/04/2025

AİHM, Avusturya/İtalya, B.No. 788/60, K.T.11/01/1961

AİHM, Banković ve Diğerleri/Belçika ve Diğerleri (B.D.), B. No. 52207/99, K.T. 12/12/2001

AİHM, Beyeler/İtalya, B.No. 33202/96, K.T. 05/01/2000

- AIHM*, Bielau/Avusturya, B. No. 20007/22, K.T.27/08/2024
- AIHM*, Big Brother Watch ve Diğerleri/B.K (1. Daire), B.No. 58170/13, K.T. 13/09/2018
- AIHM*, Big Brother Watch ve Diğerleri/B.K(B.D.), B.No. 58170/13, K.T. 25/05/2021
- AIHM*, Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi/İrlanda (B.D.), B. No. 45036/98, K.T. 30/06/2005
- AIHM*, Călin Georgescu/Romanya, B. No. 37327/24, K.T. 11/02/2025
- AIHM*, Cano Mayo/İspanya, B.No. 3142/11, K.T.11/10/2016
- AIHM*, Carter/Rusya, B. No. 20914/07, K.T. 21/09/2021 § 133-148
- AIHM*, Centrum För Rättvisa/İsveç, B. No. 35252/08, 25/05/2021
- AIHM*, Dániel Karsai/ Macaristan, B. No. 32312, K.T. 13/06/2024
- AIHM*, Danilet/Romanya, B. No. 16915/21, K.T. 20/02/2024
- AIHM*, De Becker/Belçika, B. No. 214/56, K.T. 27/03/1962
- AIHM*, De Wilde, Ooms ve Versyp/Belçika, 2832/66, K.T. 18/06/1971
- AIHM*, Delfi As/Estonya (B.D), B. No. 64569/09, K.T.16/06/2015
- AIHM*, Duarte Agostinho ve Diğerleri/Portekiz ve Diğerleri (B.D.), B.No. 39371/20, K.T.09/04/2024
- AIHM*, Ecodefence ve Diğerleri/Rusya, B. No. 9988/13, K.T. 14/06/2022
- AIHM*, Editorial Board of Pravoye Delo ve Shtekel/Ukrayna, B. No. 33014/05, K.T. 05/05/2011
- AIHM*, Gürcistan/Rusya (II) (B.D.), B.No.38263/08, K.T.21/01/2021
- AIHM*, Hirsi Jamaa ve Diğerleri/İtalya (B.D.), B. No. 27765/09, K.T. 23/02/2012
- AIHM*, Jankovskis/Litvanya, B. No. 21575/08, K.T. 17/01/2017 § 62
- AIHM*, Lawless/İrlanda(1), B. No. 332/57, K.T. 14/11/1960.
- AIHM*, Le Marrec/Fransa, B. No. 52319/22, K.T.05/11/2024
- AIHM*, Loizidou/Türkiye (B.D.), B.No:15318/89, K.T. 18/12/1996
- AIHM*, Magyar Jeti Zrt/Macaristan, B. No. 11257/16, K.T.04/12/2018
- AIHM*, Mansouri/İtalya (B.D.), B.No. 3386/16, K.T. 29/04/2025
- AIHM*, Melike/Türkiye, B.No. 35786/19, K.T.15/06/2021
- AIHM*, Mesić/Hırvatistan (No 2), B. No. 45066/17, 30/05/2023



- AIHM*, Moskal/Polonya, B.No. 10373/05, 15/09/2009
- AIHM*, Podchasov/Rusya, B.No. 33696/19, K.T.13/02/2024
- AIHM*, Roman Zakharov/ Rusya (B.D.), B. No. 47143/06, K.T. 04/12/2015
- AIHM*, Sanchez/Fransa (B.D.), B. No. 45581/15, K.T.15/05/2023
- AIHM*, Savva Terentyev/Rusya, B. No. 10692/09, K.T.28/08/2018
- AIHM*, Semenya/İsviçre (B.D.) B. No. 10934/21, K.T.10/07/2025
- AIHM*, S.S. ve Diğerleri/İtalya, B. No. 21660/18, K.T. 20/05/2025
- AIHM*, Stichting Landgoed Steenberg ve Diğerleri/ Hollanda, B. No. 19732/17, K.T. 16/02/2021
- AIHM*, Szabó ve Vissy/Macaristan, B.N. 37138/14, K.T. 12/01/2016
- AIHM*, The J. Paul Getty Trust ve Diğerleri/İtalya, B. No. 35271/19, 02/05/2024
- AIHM*, Türkiye Birleşik Komünist Partisi ve Diğerleri/Türkiye, B. No. 19392/92, K.T. 30/01/1998
- AIHM*, Verein Klimaseniorinnen Schweiz ve Diğerleri/ İsviçre (B.D), B. No. 53600/20, 09/04/2024
- BM Çocuk Hakları Komitesi*, Chiara Sacchi ve Diğerleri/ Arjantin, B. No: 104/2019, K.T.23/09/2021

