

Yeni Güç Mimarisi: Dijital Hegemonya

İmran Gürakan

Çiğdem Gizem Okkaoğlu

toplum.org.tr



Yayın Hakları ©

Bu yayının tüm hakları Toplum Çalışmaları Enstitüsü'ne aittir. Toplum Çalışmaları Enstitüsü'nden izin alınmadan yayının tümünün ya da bir kısmının herhangi bir yöntem ile basımı, yayımı, çoğaltılması ve dağıtımı yapılamaz. Kaynak göstermek şartıyla alıntı yapılabilir.

Yayın No: 27

Yayın Tarihi: 21.08.2026



TOPLUM ÇALIŞMALARI ENSTİTÜSÜ

Adres : Cevizlidere Mah. Mevlana Bulv. No:123/305 Çankaya/Ankara
Telefon : 0312 939 93 00
E-posta : info@toplum.org.tr
Website : www.toplum.org.tr

HAKKIMIZDA

Toplum Çalışmaları Enstitüsü, Türkiye'nin nitelikli insan kaynağını ülkemizin kronik yahut güncel sorun alanlarına yönelterek politik karar alıcılara rafine çözüm önerileri sunmayı ana kuruluş amacı olarak benimser. Amacına uygun olarak gerçekleştirdiği çalışmalarda, toplumumuzun genel çıkarlarının öncelenmesini esas alır. Bu esas, Toplum Çalışmaları Enstitüsü'nün zaman ve zeminden bağımsız, değişmez ilkesidir. Türkiye'nin potansiyeline uygun atılımlar için yeni jenerasyon zihinleri, fikri üretime teşvik etmek ve bu üretimi ülke birikimimize anlamlı katkılar olarak sunmak ana motivasyon kaynağıdır.

YÖNETİM KURULU

Dr. Yavuz Selim Günay, Enstitü Başkanı

Dr. Halim Alperen Çıtak, Hukuk ve Adalet Programı Direktörü

İmran Gürakan, Dijital Dönüşüm ve Girişimcilik Programı Direktörü

Doç. Dr. Asmin Kavas, Şehircilik Programı Direktörü

Yağmur Uzunırmak, Araştırma ve Veri Analizi Programı Direktörü

Yasemin Satır Çilingir, Ekonomi Programı Direktörü

Berçin Yiğitaslan, Dış Politika Programı Direktörü

Çiğdem Gizem Okkaoğlu, Enstitü Genel Sekreteri

Aykutalp Arıcı, Yönetim Kurulu Üyesi

Ahmet Oğuz Atalay, Yönetim Kurulu Üyesi

Dr. Abdullah Çağıl, Yönetim Kurulu Üyesi

Vasıf İnanç Duygulu, Yönetim Kurulu Üyesi

Gökhan Güler, Yönetim Kurulu Üyesi

Timuçin Koray Güzelderen, Yönetim Kurulu Üyesi

Nihat Yıldırım, Yönetim Kurulu Üyesi

Mustafa Gül, Yönetim Kurulu Üyesi

Yeni Güç Mimarisi: Dijital Hegemonya

**İmran Gürakan
Çiğdem Gizem Okkaoğlu**

21 Ağustos 2026

1. Giriş

1.1 Dijitalleşme ve Egemenlik İlişkisinin Dönüşümü

Dijital teknolojiler son yirmi yıl içinde yalnızca ekonomik üretim biçimlerini değil, devletlerin egemenlik kapasitesini, kamusal karar alma süreçlerini ve toplumsal ilişkilerin örgütlenme biçimini de dönüştürmüştür. Veri işleme kapasitesinin artması, bulut bilişim altyapılarının yaygınlaşması, yapay zekâ sistemlerinin günlük yaşamın merkezine yerleşmesi ve dijital platformların ekonomik faaliyetler üzerindeki belirleyici etkisi, klasik egemenlik anlayışının yeniden değerlendirilmesini zorunlu hale getirmiştir. Günümüzde devletlerin yalnızca fiziksel sınırlarını koruması yeterli görülmemektedir; aynı zamanda veri akışlarını, kritik dijital altyapıları ve algoritmik karar mekanizmalarını ne ölçüde denetleyebildiği de egemenlik kapasitesinin önemli bir unsuru olarak değerlendirilmektedir [1].

Dijitalleşme artık yalnızca ekonomik faaliyetlerin yürütüldüğü teknik bir alan değil; modern toplumların yapısal omurgası haline gelen bütüncül bir altyapıdır. Kamu hizmetlerinden finansal sistemlere, iletişim ağlarından güvenlik mimarilerine kadar geniş bir alan dijital sistemler üzerinden işlemektedir. Bu durum, dijital altyapıları ekonomik verimlilik araçlarının ötesine taşıyarak devlet kapasitesi ve kamusal düzen açısından stratejik hale getirmektedir.

Bu dönüşümün en dikkat çekici yönlerinden biri, kamusal işlevlerin giderek artan ölçüde özel teknoloji şirketlerinin altyapıları üzerinden yürütülmesidir. Kamu kurumları veri depolama hizmetleri için küresel bulut sağlayıcılarına bağımlı hale gelmekte, iletişim süreçleri uluslararası platformlar üzerinden yürütülmekte, ekonomik faaliyetlerin önemli bir bölümü dijital araçlar vasıtasıyla gerçekleşmektedir. Eğitimden sağlığa, bankacılıktan kamu güvenliğine kadar geniş bir alan, küresel teknoloji şirketlerinin geliştirdiği teknik altyapılar üzerinde işlemektedir. Bu durum, dijital teknolojilerin ekonomik bir araç olmanın ötesine geçtiğini; devlet kapasitesi, ulusal güvenlik ve toplumsal düzen açısından stratejik bir niteliğe sahip olduğunu göstermektedir.

COVID-19 pandemisi, söz konusu bağımlılık ilişkilerini daha görünür hale getirmiştir. Pandemi döneminde uzaktan eğitim sistemleri, dijital ödeme altyapıları, çevrim içi haberleşme araçları ve bulut tabanlı kamu hizmetleri toplumsal yaşamın devamlılığı açısından kritik hale gelmiştir. Böylece dijital altyapılar, elektrik, ulaşım ve enerji sistemleri gibi temel kamusal altyapılarla benzer bir stratejik konuma yerleşmiştir. Ancak bu altyapıların büyük bölümünün ulusötesi teknoloji şirketlerinin denetiminde bulunması, dijital egemenlik tartışmalarını yalnızca teknik bir mesele olmaktan çıkararak doğrudan siyasi ve hukuki bir sorun haline getirmiştir.

Bugün küresel dijital ekonominin temel katmanları sınırlı sayıdaki şirket tarafından kontrol edilmektedir. Arama motorları, mobil işletim sistemleri, uygulama mağazaları, dijital reklam altyapıları, sosyal medya ağları ve bulut hizmetleri belirli platformların yoğunlaşmış gücü altında şekillenmektedir. Google'ın küresel arama pazarındaki hâkim konumu, Apple ve Google'ın mobil işletim sistemi pazarını büyük ölçüde paylaşması, Meta'nın dijital iletişim alanındaki ağırlığı ve Amazon'un bulut altyapısındaki merkezi rolü, bu yoğunlaş-

manın en görünür örneklerini oluşturmaktadır [2]. Bu yapı, klasik piyasa yoğunlaşması tartışmalarının ötesinde, ekonomik ve siyasal karar alma süreçleri üzerinde doğrudan etkide bulunan yeni bir güç mimarisi yaratmaktadır.

Bu nedenle dijital platformların yükselişi yalnızca rekabet hukuku bağlamında değerlendirilebilecek bir mesele değildir. Mesele aynı zamanda demokratik denetim, kamusal şeffaflık, veri güvenliği ve devletlerin politika üretme kapasitesiyle doğrudan ilişkilidir. Algoritmaların hangi içeriği görünür kıldığı, hangi uygulamaların dijital pazarlara erişebildiği veya hangi verilerin hangi ülkelerin hukukuna tabi olduğu gibi sorular, artık teknik ayrıntılar değil; egemenlik ve kamusal otorite tartışmalarının merkezinde yer alan konulardır.

Bu rapor, dijital hegemonya kavramını tam da bu bağlam içinde ele almaktadır. Raporun temel argümanı, dijital platformların ekonomik güçlerinin ötesinde, devletlerin düzenleme kapasitesini ve toplumsal alanın işleyişini etkileyen yapısal bir güç konumu elde ettiğidir. Bu güç yalnızca piyasa paylarından kaynaklanmamakta; veri birikimi, ağ etkileri, altyapı bağımlılığı, algoritmik yönlendirme kapasitesi ve devletlerle kurulan stratejik ilişkiler aracılığıyla derinleşmektedir.

Dijital hegemonya kavramı bu çalışmada üç temel eksen üzerinden incelenmektedir. İlk olarak, küresel platformların ekonomik ve teknolojik güç yoğunlaşmasının hangi mekanizmalar üzerinden inşa edildiği ele alınacaktır. İkinci olarak, bu yoğunlaşmanın devlet kapasitesi, demokratik süreçler ve bireysel özerklik üzerindeki etkileri tartışılacaktır. Son olarak ise Türkiye'nin mevcut dijital bağımlılık yapısı analiz edilerek, düzenleyici kapasiteyi ve stratejik özerkliği güçlendirmeye yönelik politika seçenekleri değerlendirilecektir.

Bu çerçevede raporun temel argümanı, dijital hegemonyanın tek boyutlu bir güç olgusu olmadığıdır. Hegemonya artık birbiriyle bağlantılı üç katman üzerinden işlemektedir: Ağ etkileri, veri yoğunlaşması ve ekosistem bağımlılığı aracılığıyla inşa edilen piyasa gücü; Palantir, Microsoft ve Anduril gibi örneklerde somutlaşan devlet-teknoloji füzyonu ve CLOUD Act (ABD'nin Amerikan teknoloji şirketlerinin dünyanın herhangi bir yerinde depoladığı verilere belirli koşullarda erişim talep etmesine olanak sağlayan yasal düzenleme) gibi düzenlemeler aracılığıyla fiziksel sınırların ötesine taşınan hukuki yetki alanı genişlemesi. Bu üç katman birlikte değerlendirildiğinde dijital hegemonya, yalnızca ekonomik bir yoğunlaşma değil; jeopolitik bir mimari olarak karşımıza çıkmaktadır. Raporun temel amacı, bu mimarinin işleyişini analiz etmek ve Türkiye'nin bu yapı karşısında daha güçlü bir konuma geçebilmesi için gerekli politika önceliklerini değerlendirmektir.

Bu raporun hazırlık süreci devam ederken, dijital egemenlik gündemini doğrudan ilgilendiren önemli bir gelişme yaşanmıştır. 18 Ağustos 2026 tarihli ve 33344 sayılı Resmî Gazete'de yayımlanan 2026/9 sayılı Cumhurbaşkanlığı Genelgesi ile "Türkiye Yapay Zekâ Eylem Planı (2026-2030)" resmen yürürlüğe girmiştir. Sanayi ve Teknoloji Bakanlığı koordinasyonunda; kamu kurumları, özel sektör, üniversiteler ve sivil toplum kuruluşlarının iş birliğiyle hazırlanan Plan, 2021-2025 dönemini kapsayan Ulusal Yapay Zekâ Stratejisi'nin kazanımları üzerine inşa edilmiş; insan odaklılık, güvenilirlik, etik sorumluluk, dijital egemenlik ve sürdürülebilir kalkınma ilkelerini temel almıştır. Genelgede yapay zekânın "büyük veri, gelişmiş hesaplama kapasitesi ve algoritmik yeniliklerin birleşimiyle ortaya çıkan"

kritik bir teknoloji olarak tanımlanması ve ülkelerin rekabet gücü, verimlilik düzeyi ile teknolojik bağımsızlığının bu alandaki yetkinliklerle şekillendiğinin vurgulanması, bu raporun temel argümanıdır. Bu doğrultuda çalışmanın ilgili bölümlerinde, söz konusu Eylem Planı'nın getirdiği stratejik çerçeve, hedefler ve politika araçlarına ilişkin güncel değerlendirmelere yer verilmiştir. Planın hazırlık sürecinde; 2021-2025 Ulusal Yapay Zekâ Stratejisi ve 2024-2025 Eylem Planı'nın yanı sıra TBMM Yapay Zekâ Araştırma Komisyonu Raporu ile Cumhurbaşkanlığı Bilim, Teknoloji ve Yenilik Politikaları Kurulu'nun Ulusal Yapay Zekâ Politika Belgesi'nden yararlanıldığı; kamu, özel sektör, üniversite ve sivil toplum temsilcilerinden yaklaşık 500 profesyonelle çalıştaylar yürütüldüğü ve bir Vatandaş Görüşü Anketi aracılığıyla iki binden fazla eylem önerisinin değerlendirildiği belirtilmektedir. Bu katılımcı hazırlık zemini, planın yalnızca teknik bir yol haritası değil; aynı zamanda geniş bir toplumsal mutabakat arayışını da yansıtan bir belge olarak okunmasına imkân tanımaktadır.

1.2 Dijital Egemenlik Kavramı

Klasik egemenlik anlayışı büyük ölçüde fiziksel sınırlar ve coğrafi kontrol üzerinden şekillenmiştir. Ancak veri akışlarının sınır aşan niteliği, bulut altyapılarının küresel yapısı ve algoritmik sistemlerin kamusal alan üzerindeki etkisi, egemenlik tartışmalarını görünmeyen dijital katmanların yönetimi meselesine dönüştürmektedir.

Dijital egemenlik kavramı son yıllarda hem akademik literatürde hem de politika belgelerinde giderek daha sık kullanılan bir çerçeve haline gelmiştir. Kavram genel olarak, devletlerin dijital altyapılar, veri akışları, kritik teknolojiler ve algoritmik sistemler üzerindeki denetim kapasitesini ifade etmektedir [3]. Bununla birlikte dijital egemenlik yalnızca teknik altyapının yerli olması anlamına gelmez. Asıl mesele, devletlerin ve toplumların dijital sistemler karşısında bağımsız karar alma kapasitesini ne ölçüde koruyabildiğidir.

Bu kapsamda dijital egemenliğin ilk boyutu veri egemenliğidir. Veri, günümüz ekonominin temel stratejik kaynaklarından biri haline gelmiştir. Kamu kurumlarının, şirketlerin ve bireylerin ürettiği verilerin hangi ülkede saklandığı, hangi hukuki rejime tabi olduğu ve kimler tarafından işlenebildiği, doğrudan siyasi ve ekonomik sonuçlar doğurmaktadır. Özellikle ABD'de kabul edilen CLOUD Act düzenlemesi, Amerikan şirketlerinin yurt dışındaki verileri belirli koşullar altında ABD makamlarıyla paylaşabilmesine imkân tanımaktadır [4]. Bu durum, verinin fiziksel olarak başka bir ülkede bulunmasının tek başına egemenlik güvencesi sağlamadığını göstermektedir.

İkinci boyut, kritik dijital altyapılar üzerindeki denetim kapasitesidir. Bulut bilişim hizmetleri, mobil işletim sistemleri, arama motorları, uygulama mağazaları ve yapay zekâ modelleri gibi altyapılar, günümüz dijital ekonominin temel bileşenlerini oluşturmaktadır. Bu altyapılar üzerinde yoğunlaşan dış bağımlılık, devletlerin kriz anlarında hareket alanını daraltabilmektedir. Özellikle jeopolitik gerilimler, yaptırım süreçleri veya ticari anlaşmazlıklar sırasında kritik dijital hizmetlere erişimin kesilmesi ihtimali, dijital bağımlılığı doğrudan ulusal güvenlik meselesi haline getirmektedir.

Üçüncü boyut ise algoritmik egemenliktir. Dijital platformlar yalnızca teknik hizmet sunmamakta; aynı zamanda bilgiye erişim biçimlerini, tüketim tercihlerini ve kamusal tar-

tışma alanını da şekillendirmektedir. Arama motorları, sosyal medya platformları ve öneri sistemleri, hangi içeriğin görünür hale geleceğini büyük ölçüde belirlemektedir. Bu nedenle algoritmaların işleyişi, demokratik toplumlarda şeffaflık ve hesap verebilirlik tartışmalarının merkezine yerleşmiştir.

Dijital egemenlik tartışmaları Avrupa Birliği, Çin ve Amerika Birleşik Devletleri gibi farklı aktörlerde farklı siyasi yaklaşımlar üzerinden şekillenmektedir. Avrupa Birliği veri koruması, rekabet hukuku ve platform düzenlemeleri üzerinden düzenleyici kapasitesini güçlendirmeye çalışırken; Çin daha merkezi ve devlet kontrollü bir dijital ekosistem modeli geliştirmektedir. Amerika Birleşik Devletleri ise küresel teknoloji şirketlerinin ekonomik gücü sayesinde dijital alanda belirleyici konumunu sürdürmektedir [5]. Bu farklı modeller, dijital egemenliğin yalnızca teknik değil, aynı zamanda siyasi ve ideolojik bir tercih alanı olduğunu göstermektedir.

Türkiye açısından bakıldığında dijital egemenlik tartışması somut ve çok boyutlu bir kırılmalıklar haritasına karşılık gelmektedir. Hukuki boyutta, kamu verilerinin ABD merkezli bulut altyapılarında işlenmesi CLOUD Act kapsamında ciddi bir yetki alanı sorununa yol açmaktadır. Güvenlik boyutunda, kritik altyapıların siber korumasında yabancı sistem bağımlılığı; enerji, bankacılık ve sağlık gibi stratejik sektörlerde yapısal bir kırılmalık oluşturmaktadır. Ekonomik boyutta ise dijital reklam gelirlerinin büyük bölümünün yabancı platformlara akmasının ve platform ekonomisindeki vergi egemenliği açığının Türkiye'nin kendi topraklarında üretilen dijital değer üzerindeki denetimini zayıflattığı söylenebilecektir. Bununla birlikte 7545 sayılı Siber Güvenlik Kanunu, Ulusal Yapay Zekâ Stratejisi ve Yerli İkame Zorunluluğu, bu bağımlılıkların farkındalığının arttığını ve politika gündemine girdiğini göstermektedir. Önümüzdeki dönem, bu farkındalığın somut kurumsal ve düzenleyici kapasiteye dönüşüp dönüşmeyeceğini belirleyecektir.

Bu nedenle dijital egemenlik, dünyadan kopuşu veya tüm teknolojik sistemlerin yerleştirilmesini ifade eden bir yaklaşım olarak değerlendirilmemelidir. Daha gerçekçi yaklaşım, kritik alanlarda bağımlılıkları azaltmak, düzenleyici kapasiteyi güçlendirmek ve stratejik karar alma alanlarını koruyabilmektir. Bu raporun geri kalan bölümlerinde, dijital hegemonyanın ekonomik, hukuki ve siyasi boyutları bu çerçeve içinde ayrıntılı biçimde incelenecektir.

2. Dijital Platform Gücü ve Hegemonya Tartışmaları

2.1 Hegemonya Kavramının Dijital Alana Uyarlanması

Dijital platformların ekonomik ve toplumsal etkisini açıklamak için kullanılan en önemli kavramsal çerçevelerden biri hegemonya yaklaşımıdır. Antonio Gramsci tarafından geliştirilen hegemonya kavramı, siyasal iktidarın yalnızca zor kullanımıyla değil, rıza üretimi yoluyla da sürdürüldüğünü ileri sürmektedir [6]. Gramsci'ye göre egemenlik, yalnızca devletin hukuki veya askeri kapasitesine dayanmaz; aynı zamanda toplumun belirli düşünce biçimlerini doğal ve kaçınılmaz kabul etmesini sağlayan kültürel ve kurumsal mekanizmalar üzerinden yeniden üretilir.

Dijital platformların yükselişi, bu yaklaşımın teknoloji alanına uyarlanmasını mümkün kılmıştır. Günümüzde büyük teknoloji şirketleri yalnızca ekonomik aktörler değildir. Aynı

zamanda bilgiye erişim biçimlerini belirleyen, iletişim altyapılarını yöneten ve kullanıcı davranışlarını şekillendiren yapılar haline gelmişlerdir. Arama motorlarının hangi sonuçları öne çıkardığı, sosyal medya platformlarının hangi içerikleri görünür hale getirdiği veya uygulama mağazalarının hangi uygulamalara erişim sağladığı, kamusal alanın işleyişi üzerinde doğrudan etki yaratmaktadır.

Bu durum, dijital platformların toplumsal rızanın oluşumunda merkezi bir rol üstlendiğini göstermektedir. Özellikle algoritmik sistemlerin görünmez niteliği, platform gücünün klasik medya yapılarından farklı biçimde işlemesine yol açmaktadır. Geleneksel medya ortamında editoryal tercihler daha görünürken, dijital platformlarda içerik sıralama ve görünürlük kararları çoğu zaman kullanıcılar tarafından fark edilmeyen teknik süreçler üzerinden gerçekleşmektedir. Böylece platformların tercihleri, tarafsız teknik kararlar gibi sunulabilmektedir.

Bu nedenle dijital hegemonya yalnızca piyasa yoğunlaşmasıyla açıklanabilecek bir mesele değildir. Dijital platformlar ekonomik güçlerini kültürel etki, veri birikimi ve altyapı kontrolüyle birleştirmektedir. Bu birleşim, onları hem ekonomik hem de siyasi açıdan stratejik aktörlere dönüştürmektedir.

2.2 Platform Kapitalizmi ve Veri Ekonomisi

Dijital platformların yükselişini açıklamak için geliştirilen en etkili yaklaşımlardan biri platform kapitalizmi teorisi. Nick Srnicek'e göre platformlar, kullanıcılar arasındaki etkileşimleri organize eden ve bu etkileşimlerden veri üreten dijital araçlar olarak faaliyet göstermektedir [7]. Bu modelde ekonomik değer, yalnızca doğrudan mal veya hizmet satışından değil; kullanıcı davranışlarının sürekli biçimde izlenmesi ve analiz edilmesinden elde edilmektedir.

Platform ekonomisinin merkezinde veri yer almaktadır. Kullanıcıların yaptığı aramalar, satın alma tercihleri, sosyal ilişkileri, konum bilgileri ve çevrim içi davranışları, platformlar açısından stratejik bir ekonomik kaynak niteliği taşımaktadır. Veri birikimi arttıkça algoritmaların doğruluğu ve hizmet kalitesi yükselmekte; bu durum daha fazla kullanıcı çekerek yeni veri üretimini teşvik etmektedir. Böylece kendini besleyen bir ekonomik döngü ortaya çıkmaktadır.

Bu yapı, geleneksel sanayi ekonomisinden önemli ölçüde farklıdır. Sanayi ekonomisinde ölçek ekonomileri üretim kapasitesine dayanırken, dijital ekonomide ölçek avantajı veri yoğunlaşmasından kaynaklanmaktadır. Platformların rekabet üstünlüğü yalnızca finansal güçlerinden değil; uzun yıllar boyunca biriktirdikleri kullanıcı verilerinden beslenmektedir. Bu nedenle yeni aktörlerin piyasaya girişi teknik olarak mümkün olsa bile, anlamlı ölçekte rekabet yaratmaları son derece güç hale gelmektedir.

Shoshana Zuboff'un geliştirdiği gözetim kapitalizmi yaklaşımı, bu ekonomik yapının toplumsal boyutunu açıklamaktadır [8]. Zuboff'a göre dijital platformlar yalnızca kullanıcı davranışlarını gözlemlemekle kalmamakta; aynı zamanda bu davranışları tahmin etmeye ve yönlendirmeye çalışmaktadır. Reklam teknolojileri sektörünün temel işleyişi de bu mantığa dayanmaktadır. Kullanıcıların gelecekte hangi ürünü satın alma, hangi içeriğe tıklama

veya hangi siyasi mesaja tepki verme ihtimalinin daha yüksek olduğunu öngörmek, platform ekonomisinin temel değer üretim mekanizmasına dönüşmüştür.

Bu nedenle veri ekonomisi yalnızca ticari bir faaliyet alanı değildir. Aynı zamanda bireysel özerklik, mahremiyet ve demokratik süreçler üzerinde doğrudan etkileri bulunan yapısal bir güç alanıdır.

2.3 Ağ Etkileri ve Piyasa Yoğunlaşması

Dijital platform ekonomilerinde piyasa yoğunlaşmasını hızlandıran en önemli mekanizmalardan biri ağ etkileridir. Ağ etkisi, bir hizmetin değerinin kullanıcı sayısı arttıkça yükselmesi anlamına gelmektedir [9]. Sosyal medya platformları bu durumun en belirgin örneklerinden biridir. Bir platformda ne kadar fazla kullanıcı varsa, o platformun diğer kullanıcılar açısından cazibesi de o ölçüde artmaktadır.

Ağ etkileri, dijital piyasalarda kazananın büyük ölçüde tüm pazarı kontrol ettiği yapılar zemin hazırlamaktadır. Kullanıcıların yoğun biçimde tercih ettiği platformlar daha fazla veri toplamakta, daha fazla reklam geliri elde etmekte ve yeni teknolojilere daha fazla yatırım yapabilmektedir. Bu süreç zaman içinde rekabetçi avantajı kalıcı hale getirmektedir.

Piyasa yoğunlaşmasını güçlendiren ikinci unsur ise kilitlenme etkisidir. Kullanıcıların bir platformdan başka bir platforma geçmesi çoğu zaman yalnızca teknik bir değişiklik anlamına gelmemektedir. Sosyal bağlantılar, geçmiş veriler, dijital arşivler ve kullanıcı alışkanlıkları belirli platformlar etrafında birikmektedir. Bu nedenle alternatif hizmetler teknik olarak mevcut olsa bile, kullanıcıların platform değiştirme maliyeti yüksek hale gelmektedir [10].

Mobil işletim sistemleri ve uygulama mağazaları bu yapının en güçlü örneklerinden biridir. Apple ve Google'ın mobil ekosistemler üzerindeki hakimiyeti, yalnızca teknik kaliteyle açıklanamaz. Uygulama dağıtım altyapılarının, ödeme sistemlerinin ve geliştirici ekosistemlerinin aynı yapı içinde bütünleşmesi, piyasaya giriş engellerini son derece yükseltmektedir.

Bu nedenle dijital platform piyasalarında klasik rekabet hukuku araçlarının çoğu zaman yetersiz kaldığı yönünde güçlü bir akademik tartışma bulunmaktadır. Özellikle Avrupa Birliği'nin Dijital Piyasalar Yasası (DMA) ile birlikte benimsediği *ex ante* düzenleme yaklaşımı, tam da bu yapısal yoğunlaşma sorunlarına müdahale etmeyi amaçlamaktadır [11].

2.4 Dijital Altyapıların Stratejik Niteliği

Dijital platformların ekonomik gücü, zaman içinde kritik altyapı niteliği taşıyan bir yapıya dönüşmüştür. Bulut bilişim hizmetleri, arama motorları, sosyal medya ağları, mobil işletim sistemleri ve yapay zekâ modelleri, modern ekonominin temel işleyiş katmanları haline gelmiştir. Kamu kurumları, finans sektörü, eğitim sistemleri ve ticari işletmeler bu altyapılar olmaksızın faaliyetlerini sürdüremeyecek ölçüde dijital sistemlere bağımlı hale gelmiştir.

Bu durum, dijital altyapıları enerji ve ulaşım altyapılarıyla benzer stratejik bir konuma taşımaktadır. Ancak dijital altyapıların önemli bir farkı bulunmaktadır: Bu altyapıların bü-

yük bölümü kamu otoriteleri tarafından değil, özel teknoloji şirketleri tarafından işletilmektedir. Böylece ekonomik faaliyetlerin ve kamusal iletişimin temel katmanları, demokratik denetim mekanizmalarının dışında şekillenebilmektedir.

Özellikle bulut bilişim alanındaki yoğunlaşma dikkat çekicidir. Amazon Web Services, Microsoft Azure ve Google Cloud gibi şirketler, küresel bulut altyapısının büyük bölümünü kontrol etmektedir [12]. Kamu kurumları ve özel şirketler kritik verilerini bu altyapılar üzerinde depolamakta; yazılım sistemlerini bu servisler aracılığıyla yürütmektedir. Bu yapı, teknik bağımlılığı aynı zamanda siyasi ve hukuki bağımlılığa dönüştürmektedir.

Benzer şekilde yapay zekâ modellerinin geliştirilmesi de giderek daha yoğun sermaye ve veri gerektiren bir alan haline gelmiştir. Büyük dil modellerinin eğitimi için gerekli işlem kapasitesi ve veri setleri, yalnızca sınırlı sayıdaki küresel şirketin erişebildiği kaynaklara dayanmaktadır. Böylece yapay zekâ alanında da yoğunlaşmış bir teknolojik güç yapısı ortaya çıkmaktadır.

Bu nedenle dijital altyapıların düzenlenmesi, yalnızca ekonomik rekabet meselesi olarak ele alınamaz. Mesele aynı zamanda kamusal denetim, demokratik hesap verebilirlik ve stratejik özerklik sorunudur. Devletlerin dijital kapasitesi ile küresel platformların ekonomik gücü arasındaki ilişki, önümüzdeki dönemin en önemli düzenleyici tartışmalarından birini oluşturmaktadır.

3. Dijital Platformların Güç Mekanizmaları

3.1 Varsayılan Ayarlar ve Davranışsal Yönlendirme

Dijital platformların piyasa gücünü sürdürmesinde teknik üstünlük kadar davranışsal ekonomi mekanizmaları da önemli rol oynamaktadır. Özellikle varsayılan ayarlar (*default settings*), kullanıcı tercihlerini biçimlendiren en etkili araçlardan biri haline gelmiştir. Davranışsal ekonomi literatürü, kullanıcıların önemli bir bölümünün mevcut ayarı değiştirmeme eğiliminde olduğunu göstermektedir [13]. Bu nedenle bir hizmetin cihazlarda veya yazılımlarda varsayılan seçenek olarak sunulması, kullanıcı davranışı üzerinde doğrudan belirleyici etki yaratmaktadır.

Mobil işletim sistemleri ve internet tarayıcıları bu durumun en görünür örneklerini oluşturmaktadır. Bir arama motorunun veya internet tarayıcısının cihazda önceden tanımlı biçimde sunulması, kullanıcıların büyük bölümünün alternatif hizmetlere yönelmemesine yol açmaktadır. ABD Adalet Bakanlığı tarafından Google hakkında yürütülen soruşturmalar kapsamında ortaya çıkan belgeler, şirketin varsayılan arama motoru statüsünü koruyabilmek için milyarlarca dolarlık anlaşmalar yaptığını göstermiştir [14]. Bu durum, varsayılan ayarların basit bir kullanıcı deneyimi tercihi değil; doğrudan ekonomik değer üreten stratejik bir araç olduğunu ortaya koymaktadır.

Varsayılan ayarlar yalnızca arama motorlarıyla sınırlı değildir. Mobil uygulama mağazaları, dijital asistanlar, harita hizmetleri, e-posta uygulamaları ve ödeme sistemleri de benzer mekanizmalar üzerinden çalışmaktadır. Kullanıcının ilk temas kurduğu hizmetin platform sahibi tarafından belirlenmesi, rekabetin başlangıç noktasını yapısal biçimde etkilemektedir.

Bu nedenle son yıllarda rekabet hukuku tartışmalarında seçim ekranı (*choice screen*) uygulamaları önem kazanmıştır. Avrupa Birliği'nin Android soruşturmaları kapsamında gündeme gelen seçim ekranı yaklaşımı, kullanıcıların ilk kurulum aşamasında alternatif hizmetler arasında aktif tercih yapmasını amaçlamaktadır [15]. Bu tür müdahaleler, dijital piyasalarda görünürde mevcut olan ancak pratikte işlemeyen rekabet koşullarını yeniden tesis etmeye yönelik araçlar olarak değerlendirilmektedir.

3.2 Ön Yükleme Stratejileri ve Veri Birikimi

Dijital platformların güç yoğunlaşmasını pekiştiren ikinci temel mekanizma ön yükleme uygulamalarıdır. Mobil cihaz üreticileri ile platform şirketleri arasında yapılan anlaşmalar sonucunda belirli uygulamalar cihazlara önceden yüklenmiş biçimde sunulmaktadır. Kullanıcıların önemli bölümü bu uygulamaları kaldırmamakta veya alternatif hizmet arayışına girmemektedir.

Avrupa Komisyonu'nun Google Android kararı, bu konuda en kapsamlı örneklerden birini oluşturmaktadır [15]. Kararda Google'ın Android işletim sistemi lisanslarını belirli uygulamaların önceden yüklenmesi şartına bağladığı tespit edilmiştir. Böylece arama motoru, internet tarayıcısı ve diğer Google hizmetleri cihazların standart bileşeni haline gelmiştir.

Ön yükleme uygulamalarının ekonomik etkisi yalnızca kullanıcı sayısı ile sınırlı değildir. Daha fazla kullanıcı, daha fazla veri üretimi anlamına gelmektedir. Veri miktarının artması ise algoritmaların gelişmesini ve hizmet kalitesinin yükselmesini sağlamaktadır. Böylece kullanıcı yoğunluğu ile veri birikimi arasında kendini güçlendiren bir döngü ortaya çıkmaktadır.

Bu durum özellikle yapay zekâ sistemleri açısından kritik hale gelmiştir. Büyük dil modelleri ve öneri sistemleri yüksek miktarda kullanıcı verisiyle beslenmektedir. Veri birikimi arttıkça sistemlerin performansı yükselmekte; performans yükseldikçe daha fazla kullanıcı çekilmektedir. Bu nedenle dijital platformların veri avantajı, zaman içinde kapanması güç yapısal bir rekabet üstünlüğüne dönüşmektedir.

Akademik literatürde bu süreç çoğu zaman “veri yoğunlaşması” ve “geri besleme döngüsü” kavramlarıyla açıklanmaktadır [16]. Yeni aktörlerin piyasaya giriş yapabilmesi teknik olarak mümkün olsa bile, uzun yıllar boyunca oluşmuş veri birikimine erişememeleri ciddi dezavantaj yaratmaktadır. Böylece piyasa yoğunlaşması yalnızca finansal kaynaklarla değil, veri altyapısı üzerinden de yeniden üretilmektedir.

3.3 Dijital Reklam Ekosistemi ve Veri Gücü

Dijital platform ekonomisinin merkezinde reklam teknolojileri sektörü bulunmaktadır. Özellikle Google ve Meta gibi şirketlerin ekonomik modeli büyük ölçüde reklam gelirlerine dayanmaktadır. Bu yapı, kullanıcı verilerinin ekonomik değere dönüştürülmesinin en gelişmiş örneklerinden birini oluşturmaktadır.

Dijital reklamcılık sistemi geleneksel medya reklamcılığından farklı olarak gerçek zamanlı veri işleme mekanizmaları üzerinden çalışmaktadır. Kullanıcının çevrim içi davranışları, ilgi alanları, konum bilgileri ve geçmiş tercihleri analiz edilmekte; reklam gösterimleri

milisaniyeler içinde gerçekleştirilen açık artırmalar aracılığıyla belirlenmektedir. Böylece reklam verenler, belirli kullanıcı profillerine son derece hassas hedefleme yöntemleriyle ulaşabilmektedir.

Bu sistemin en önemli özelliği, aynı şirketlerin reklam ekosisteminin farklı katmanlarını aynı anda kontrol etmesidir. Google hem reklam satın alma araçlarını hem yayıncı altyapılarını, hem reklam değişim platformlarını hem de kullanıcı verisinin önemli bölümünü kontrol etmektedir [17]. Bu durum, rekabet hukuku açısından ciddi çıkar çatışması tartışmalarına yol açmaktadır.

Bir şirketin hem piyasanın altyapısını işletmesi hem de bu altyapı üzerinde faaliyet gösteren aktörlerden biri olması, tarafsız rekabet koşullarını zayıflatmaktadır. Reklam teknolojileri alanında yürütülen soruşturmanın önemli bölümü, tam da bu dikey bütünleşme yapısından kaynaklanmaktadır.

Dijital reklam ekosisteminin ikinci önemli sonucu medya ekonomisi üzerinde ortaya çıkmaktadır. Reklam gelirlerinin büyük bölümünün küresel platformlarda yoğunlaşması, geleneksel medya kuruluşlarının ekonomik sürdürülebilirliğini zayıflatmaktadır. Haber kuruluşları içerik üretmeye devam ederken, reklam gelirlerinin önemli kısmı içeriği dağıtan platformlara yönelmektedir. Böylece dijital platformlar yalnızca reklam piyasasını değil, kamusal bilgi akışının ekonomik temelini de kontrol eder hale gelmektedir.

3.4 Ekosistem Entegrasyonu ve Bağımlılık İlişkileri

Büyük teknoloji şirketlerinin güç yoğunlaşmasını sürdürebilmesinde ekosistem entegrasyonu önemli rol oynamaktadır. Ekosistem yaklaşımı, farklı dijital hizmetlerin birbirine entegre edilerek kullanıcıların aynı yapı içinde tutulmasını amaçlamaktadır. E-posta hizmetleri, bulut depolama sistemleri, mobil cihazlar, ödeme altyapıları, mesajlaşma uygulamaları ve uygulama mağazaları bu bütünleşik yapının parçaları olarak çalışmaktadır.

Apple ekosistemi bu modelin en güçlü örneklerinden biridir. iPhone, iCloud, App Store, Apple Watch ve iMessage gibi hizmetler birbirine yüksek düzeyde entegre edilmiştir. Benzer şekilde Google ekosistemi de Android, Chrome, Gmail, Drive, YouTube ve Google Search gibi hizmetler üzerinden bütünleşik bir yapı oluşturmaktadır.

Ekosistem entegrasyonu kullanıcı deneyimi açısından avantajlar sunmakla birlikte, aynı zamanda bağımlılık ilişkileri yaratmaktadır. Kullanıcıların bir hizmetten ayrılması yalnızca tek bir uygulamayı bırakmak anlamına gelmemekte; bütün dijital alışkanlıklarını ve veri arşivlerini başka bir sisteme taşımalarını gerektirmektedir. Bu durum platform değiştirme maliyetini önemli ölçüde yükseltmektedir.

Benzer bağımlılık ilişkileri şirketler ve kamu kurumları açısından da ortaya çıkmaktadır. Özellikle bulut bilişim altyapılarına dayalı çalışan kurumlar, zaman içinde belirli sağlayıcılara teknik olarak bağımlı hale gelebilmektedir. Yazılım sistemlerinin, veri depolama süreçlerinin ve güvenlik altyapılarının aynı servis sağlayıcı üzerinde yoğunlaşması, alternatif sistemlere geçişi maliyetli hale getirmektedir.

Bu nedenle dijital platform gücü yalnızca piyasa payları üzerinden değerlendirilemez. Asıl mesele, kullanıcıların, şirketlerin ve kamu kurumlarının dijital yaşamlarının ne ölçü-

de belirli platformlar etrafında örgütlendiğidir. Ekosistem bağımlılığı arttıkça platformların ekonomik ve siyasi etkisi de derinleşmektedir.

3.5 Devletler ve Teknoloji Şirketleri Arasındaki Yakınlaşma

Son yıllarda dijital platformlar ile devlet kurumları arasındaki ilişkiler yeni bir boyut kazanmıştır. Özellikle yapay zekâ, büyük veri analizi ve bulut bilişim alanlarında faaliyet gösteren şirketler, kamu güvenliği ve savunma politikalarının önemli aktörleri haline gelmektedir.

Palantir Technologies bu dönüşümün en dikkat çekici örneğini oluşturmaktadır. Şirketin geliştirdiği Gotham ve Foundry platformları, farklı kaynaklardan gelen yapılandırılmamış verileri gerçek zamanlı olarak birleştirerek analitik katmana dönüştürmekte; böylece istihbarat değerlendirmesinden operasyonel karar desteğine kadar geniş bir alanda kullanılabilir. ABD Savunma Bakanlığı, CIA ve FBI başta olmak üzere pek çok federal kurum Palantir altyapısına yapısal biçimde bağımlı hale gelmiştir [18]. Bu bağımlılık ilişkisi zamanla daha derin bir boyut kazanmaktadır: Palantir, yalnızca kurumların kullandığı bir araç olmaktan çıkmakta; kurumsal hafızanın, analitik alışkanlıkların ve nihayetinde politika tercihlerinin biçimlendiği bir zemin haline gelmektedir. Hangi verinin görünür kılındığı, hangi kalıpların anlamlı sayıldığı ve hangi senaryoların karar masasına taşındığı artık kısmen bu platformların tasarım tercihlerine bağlı hale gelmektedir. Bu yapı, şirketin devletin karar alma mekanizmasıyla biçimsel olmayan ama derin bir ilişki kurduğunu; politikalara doğrudan değil, sınırları çizme kapasitesi üzerinden yön verdiğini göstermektedir.

Ancak Palantir, daha geniş bir ilişki ağının yalnızca en görünür halkasıdır. Microsoft, JWCC (Joint Warfighting Cloud Capability) çerçevesinde Pentagon'un bulut altyapısının temel sağlayıcısı konumunu sürdürmektedir. Amazon Web Services, CIA ve diğer istihbarat kurumlarına yönelik sınıflandırılmış veri işleme altyapısını işletmektedir. Google ise 2018 yılında insansız hava araçlarına yönelik görüntü analizi için geliştirilen Project Maven'dan çalışan baskısı sonucunda çekilmek zorunda kalmış; bu süreç, teknoloji şirketlerinin savunma sektörüyle ilişkisinin içeriden de tartışmalı olduğunu açıkça ortaya koymuştur [19, 20, 21]. Söz konusu örnekler yalnızca bireysel sözleşme kararlarını yansıtmamaktadır; teknoloji şirketi ile devlet arasındaki sınırın yapısal olarak bulanıklaştığı yeni bir ilişki biçimini gözler önüne sermektedir.

Bu örüntü son dönemde yeni bir aşamaya taşınmaktadır. Palantir, Anduril Industries öncülüğünde bir araya gelen ve “yeni savunma teknolojisi konsorsiyumu” olarak nitelenen yapının içinde yer almaktadır. Bu konsorsiyum, Silikon Vadisi merkezli şirketlerin geleneksel savunma yüklenicilerinin (Lockheed Martin, Raytheon gibi) yerini almak üzere Pentagon ihalelerinde ortak teklif sunan bir güç odağına dönüşmektedir [22]. Palantir aynı zamanda yazılım platformlarını insansız hava araçları ve stratosferik istihbarat alanında faaliyet gösteren şirketlerle, Performance Drone Works, Ondas ve World View dahil, doğrudan entegre etmektedir [23]. Böylece ortaya çıkan yapı yalnızca ticari bir tedarik zinciri değildir. Ortak Ar-Ge kapasitesi, bütünleşik veri altyapısı ve koordineli lobi gücüyle donatılmış; devletin savunma ve güvenlik politikalarını fiilen biçimlendirme kapasitesine sahip paralel bir karar alma odağına dönüşmektedir.

Bu gelişmeler, dijital hegemonya kavramının yalnızca platform ekonomisi veya veri yoğunlaşması üzerinden değerlendirilemeyeceğini göstermektedir. Büyük teknoloji şirketlerinin birbirleriyle oluşturdukları konsorsiyumlar, güçlenen lobi yapıları ve devlet kurumlarıyla kurulan derin entegrasyon ilişkileri, hegemonyanın bir üst düzey örgütlenmesinin yapı taşlarını oluşturmaktadır. Özel mülkiyete ait altyapıların devlet kapasitesinin ayrılmaz bir parçası haline gelmesi; şirket satın almaları, yaptırımlar veya siyasi krizler sırasında bu bağımlılık ilişkilerini kritik bir kırılma noktasına dönüştürmektedir. Dahası, özel şirketlerin kâr güdüsü ile ulusal güvenlik çıkarlarının her zaman örtüşmeyeceği gerçeği, demokratik toplumlarda bu ilişkinin hangi denetim mekanizmaları çerçevesinde yürütüleceğine dair köklü sorular doğurmaktadır.

Bu nedenle dijital hegemonya tartışmaları yalnızca ekonomik yoğunlaşma ekseninde değerlendirilemez. Mesele aynı zamanda devlet kapasitesi, ulusal güvenlik ve jeopolitik güç dengeleriyle; giderek daha da önemlisi, demokratik denetimin sınırlarıyla doğrudan bağlantılıdır.

4. Devlet, Güvenlik ve Dijital Egemenlik

4.1 Dijital Altyapıların Ulusal Güvenlik Boyutu

Dijital teknolojilerin ekonomik ve toplumsal yaşamın merkezine yerleşmesi, bu altyapıların ulusal güvenlik perspektifiyle değerlendirilmesini zorunlu hale getirmiştir. Günümüzde kamu hizmetlerinin önemli bölümü dijital sistemler üzerinden yürütülmektedir. Vergi sistemleri, sağlık altyapıları, bankacılık hizmetleri, enerji şebekeleri, iletişim ağları ve kamu veri tabanları büyük ölçüde dijital platformlara bağımlı hale gelmiştir. Özellikle enerji, ulaşım ve su altyapıları gibi fiziksel sistemlerin dijital ağlarla bütünleşmesi, “siber-kinetik güvenlik” tartışmalarını daha önemli hale getirmektedir. Siber saldırılar artık yalnızca veri güvenliğini değil; fiziksel altyapıların işleyişini de doğrudan etkileyebilmektedir. Bu nedenle dijital altyapılarda yaşanabilecek kesintiler veya dış müdahaleler, yalnızca teknik sorunlar değil; devlet kapasitesini doğrudan etkileyebilecek stratejik riskler olarak görülmektedir.

Siber güvenlik literatürü, kritik altyapıların korunmasını modern devletlerin temel güvenlik öncelikleri arasında değerlendirmektedir [24]. Özellikle bulut bilişim sistemlerinin yaygınlaşmasıyla birlikte, devlet kurumlarının ve özel sektörün verileri uluslararası teknoloji şirketlerinin altyapılarında depolanmaya başlamıştır. Bu durum maliyet ve verimlilik açısından önemli avantajlar sunsa da, aynı zamanda yeni bağımlılık ilişkileri yaratmaktadır.

Küresel bulut altyapısının büyük bölümünün sınırlı sayıda şirket tarafından kontrol edilmesi, dijital egemenlik tartışmalarını derinleştirmiştir. Amazon Web Services, Microsoft Azure ve Google Cloud gibi şirketler yalnızca ticari hizmet sağlayıcıları değildir; aynı zamanda devletlerin ve şirketlerin dijital faaliyetlerini sürdürebildiği temel altyapıları işletmektedir [12, 25]. Bu altyapılar üzerindeki yoğunlaşma, teknik bağımlılığı aynı zamanda siyasi ve hukuki bağımlılığa dönüştürmektedir.

Literatürde son yıllarda tartışılan “*kill switch*” riski, kritik dijital hizmetlerin belirli şirketler veya yabancı altyapılar tarafından tek taraflı biçimde sınırlandırılabilmesi ihtimaline işaret etmektedir. Bulut altyapıları, uygulama mağazaları veya temel dijital servisler üze-

rindeki yüksek yoğunlaşma, jeopolitik kriz dönemlerinde ekonomik ve kamusal faaliyetler açısından sistemik kırılganlık yaratabilmektedir.

Özellikle jeopolitik krizler ve yaptırım süreçleri sırasında dijital altyapı bağımlılığının etkileri daha görünür hale gelmektedir. Kritik yazılım hizmetlerine erişimin kısıtlanması, lisans iptalleri veya veri erişimi konusundaki hukuki anlaşmazlıklar, devletlerin dijital kapasitesini doğrudan etkileyebilmektedir. Bu nedenle dijital altyapıların güvenliği yalnızca siber saldırılara karşı korunma meselesi değildir; aynı zamanda stratejik özerklik ve kriz yönetimi kapasitesiyle ilişkilidir.

4.2 Veri Egemenliği ve Yetki Alanı Tartışmaları

Dijital egemenlik tartışmalarının en kritik hukuki boyutlarından biri, verinin nerede depolandığından bağımsız olarak kimin erişim hakkına sahip olduğu sorusudur. Geleneksel hukuk sistemlerinde yetki alanı fiziksel sınırlar üzerinden tanımlanmaktaydı. Ancak dijital veri akışlarının sınır aşan niteliği, bu yaklaşımı köklü biçimde karmaşık hale getirmiştir.

Amerika Birleşik Devletleri'nde 2018 yılında yürürlüğe giren CLOUD Act bu dönüşümün en çarpıcı hukuki örneğini oluşturmaktadır [4]. Düzenleme, Amerikan şirketlerinin kontrolündeki verilerin fiziksel olarak başka ülkelerde bulunsu dahi belirli koşullar altında ABD makamlarına sunulabilmesini mümkün kılmaktadır. Böylece bir kamu kurumunun veya şirketin verisi, ABD merkezli bir bulut sağlayıcısı üzerinde tutulduğu sürece ABD hukukunun erişim alanına girebilmektedir. Bu durum, verinin fiziksel konumunun tek başına egemenlik güvencesi sağlamadığını açıkça ortaya koymaktadır.

Ancak CLOUD Act, tek başına değerlendirildiğinde eksik bir sonuca yönlendirir. Söz konusu düzenleme, ABD'nin daha geniş bir teknoloji gücü stratejisinin hukuki ifadesidir. Bu strateji birkaç katmandan oluşmaktadır. Bir yanda özgürlük söylemi ve açık ekosistem modeliyle küresel teknoloji gelişimini kendi bünyesinde besleyen; dünyanın dört bir yanından yetkin araştırmacıları ve girişimcileri çeken bir sistem bulunmaktadır. Öte yanda bu sistemin ürettiği altyapı küreselleştikçe ABD hukukunun yetki alanı da genişlemektedir: Platform ihraç ettiğinizde, egemenlik alanınızı da ihraç etmiş olursunuz. Son dönemde ise bu ilişki daha doğrudan bir boyut kazanmaktadır. Gelişmiş yarı iletken ihracatını kısıtlayan ticaret kontrolleri, Huawei'ye yönelik tedarik zinciri yasakları ve yapay zekâ alanını düzenleyen yürütme kararları, teknolojinin artık açıkça jeopolitik bir araç olarak konumlandırıldığını göstermektedir [26].

Çin bu tablonun karşı kutbunu oluşturmaktadır; ancak model temelden farklıdır. ABD'de devlet büyük ölçüde özel şirketlerin çıkarlarını korurken, Çin'de özel şirketler devletin aracına dönüşmektedir. 2017 tarihli Ulusal İstihbarat Kanunu, tüm Çinli kuruluşların talep halinde devletle istihbarat iş birliği yapmasını zorunlu kılmaktadır [27]. Buna ek olarak Askeri-Sivil Füzyon politikası çerçevesinde sivil teknoloji geliştirme faaliyetleri yasal olarak askeri amaçlarla entegre edilebilmektedir [28]. 2021 tarihli Veri Güvenliği Kanunu ise CLOUD Act'in tam ters yönde çalışmaktadır: Yabancı tarafların Çin verisine erişimini engellerken Çin'in kendi veri çıkışını sıkı biçimde kontrol altında tutmaktadır. Huawei ve ZTE üzerinden yürütülen küresel telekomünikasyon altyapısı yayılımı da bu çerçevede değer-

lendirilmektedir, teknik altyapı ihraç edilirken veri akışları üzerindeki denetim potansiyeli de beraberinde taşınmaktadır.

Avrupa Birliği bu iki model karşısında farklı bir konum sahiplenmiştir. Küresel ölçekte rekabet edebilecek teknoloji platformlarından yoksun olan AB, ekonomik büyüklüğünü standart belirleyici bir güce dönüştürme stratejisini benimsemiştir. Akademik literatürde “Brüksel Etkisi” olarak kavramsallaştırılan bu yaklaşım [29], büyük pazar erişimini bir kaldıraç olarak kullanmakta; küresel teknoloji şirketlerini AB standartlarına uymak zorunda bırakmaktadır. GDPR’nin veri aktarımına getirdiği kısıtlamalar bu stratejinin en etkili aracı olmuştur. Avrupa Birliği Adalet Divanı’nın Schrems II kararı, ABD’ye veri aktarımını fiilen askıya almış; Amerikan şirketlerini veri işleme modellerini yeniden yapılandırmak zorunda bırakmıştır [30]. Bununla birlikte AB’nin yalnızca düzenlemeyle yetinmenin sınırlarına ulaştığı görülmektedir. Gaia-X ve EuroStack girişimleri, teknolojik üretim kapasitesi olmadan normatif gücün uzun vadede sürdürülemeyeceğinin farkındalığını yansıtmaktadır.

Rusya ise bu tabloda ayrı bir vaka oluşturmaktadır. Savaş öncesinde RuNet altyapısı ve SORM gözetim sistemi aracılığıyla zaten iç interneti izole etmeye yönelik Rusya, yaptırımlar sonrasında bu içe kapanmayı derinleştirmiştir. Küresel teknoloji ihraç kapasitesi büyük ölçüde zayıflamış olsa da siber saldırı kapasitesi ve dezenformasyon altyapısı üzerinden teknolojinin asimetrik bir güç aracı olarak kullanımı sürmektedir. Bu durum, veri egemenliği tartışmalarında teknolojik yetkinliğin ihraç gücüyle, saldırı kapasitesinin ise ayrı bir değişken olarak değerlendirilmesi gerektiğini göstermektedir.

Bu küresel tablo, Türkiye açısından somut bir hukuki çerçeve sorusu doğurmaktadır. Türk kamu kurumlarının ve özel sektörün önemli bölümü ABD merkezli bulut altyapılarına bağımlı durumdadır. Bu bağımlılık, CLOUD Act kapsamında söz konusu verilerin ABD hukuki süreçlerine konu olabileceği anlamına gelmektedir. Türkiye’nin 6698 sayılı KVKK’sı temel bir çerçeve sunmakla birlikte, sınır ötesi veri akışları, yabancı bulut sağlayıcılarının denetimi ve kritik kamu verilerinin işlenmesine ilişkin mekanizmalar henüz yeterli olgunluğa ulaşmamıştır. Düzenleyici kurumlar arasındaki koordinasyon eksikliği bu sorunu derinleştirmektedir. Türkiye’nin bu alanda karşı karşıya olduğu asıl mesele, yalnızca bir veri koruma kanununun varlığı değil; küresel veri güç mücadelesinde hangi tarafın hukukuna fiilen tabi olunduğudur.

4.3 Yapay Zekâ ve Jeopolitik Rekabet

Yapay zekâ teknolojileri son yıllarda küresel güç rekabetinin temel alanlarından biri haline gelmiştir. Büyük dil modelleri, veri analiz sistemleri ve otomasyon teknolojileri yalnızca ekonomik verimlilik araçları olarak görülmemekte; aynı zamanda askeri, stratejik ve siyasi kapasite unsurları olarak değerlendirilmektedir [31].

Amerika Birleşik Devletleri ile Çin arasındaki teknoloji rekabeti bu dönüşümün en belirgin örneğini oluşturmaktadır. Ancak bu rekabetin yalnızca model performansı veya araştırma yetkinliği üzerinden değerlendirilmesi yetersiz kalacaktır. Asıl mücadele hesaplama altyapısı üzerinde şekillenmektedir. Gelişmiş yarı iletken çiplere erişim, yapay zekâ modellerinin eğitilmesinde belirleyici bir darboğaz haline gelmiş; bu durum ABD’yi teknolojiyi

doğrudan bir jeopolitik araç olarak konumlandırmaya yöneltmiştir. 2022 yılında başlayan ve giderek derinleşen ihracat kısıtlamaları kapsamında Nvidia'nın en gelişmiş çipleri Çin pazarından çekilmiş; her yeni kısıtlama dalgasıyla birlikte Çin'in erişebildiği hesaplama kapasitesinin sınırlandırılması hedeflenmiştir [26]. Bununla birlikte bu politikanın sınırları da görünür hale gelmiştir: Çinli yapay zekâ şirketi DeepSeek, Ocak 2025'te kısıtlanmış donanım ile ABD'nin önde gelen modellerine yakın performans sergileyen bir sistem geliştirmiş; bu gelişme ABD teknoloji hisselerinde tek günde yaklaşık 600 milyar dolarlık piyasa değeri kaybına yol açmıştır [32]. DeepSeek vakası, donanım kısıtlamalarının tek başına hesaplama gücü rekabetini kontrol altına almaya yetmediğini; algoritma ve mimari yeniliklerin bu denklemi karmaşıktırdığını göstermektedir.

Bu süreçte büyük teknoloji şirketleri ile devletler arasındaki ilişki de yeniden şekillenmektedir. Yapay zekâ şirketleri yalnızca ticari faaliyet yürüten özel aktörler olmaktan çıkmakta; kamu güvenliği, savunma ve istihbarat politikalarının önemli bileşenleri haline gelmektedir. OpenAI, Microsoft, Google ve benzeri şirketlerin devlet kurumlarıyla geliştirdiği iş birlikleri teknoloji sektörünün jeopolitik önemini artırmaktadır [33]. Bu ilişki demokratik toplumlarda özel şirketin kâr güdüsü ile kamu yararı arasındaki gerilimi de beraberinde getirmekte; hangi yapay zekâ kararlarının kamuoyuna açık denetim mekanizmalarına tabi tutulacağı sorusunu güncel bir yönetim meselesine dönüştürmektedir.

Yapay zekâ alanındaki yoğunlaşma, aynı zamanda veri ve işlem kapasitesi yoğunlaşmasını da beraberinde getirmektedir. Büyük yapay zekâ modellerinin geliştirilmesi yüksek miktarda veri, enerji ve donanım gerektirmektedir. Bu durum yalnızca sınırlı sayıdaki şirketin küresel ölçekte rekabet edebilmesine imkân tanımakta; yapay zekâ ekosistemini yoğun sermaye gerektiren stratejik bir teknoloji alanına dönüştürmektedir [33]. Bununla birlikte DeepSeek örneği, bu yoğunlaşmanın mutlak olmadığını ve algoritmik verimlilik üzerinden kısmi dengeleyici dinamiklerin ortaya çıkabileceğini de göstermektedir.

Avrupa Birliği'nin Yapay Zekâ Yasası girişimi, bu teknolojilerin yalnızca ekonomik değil; toplumsal ve siyasi etkileri bulunduğu yaklaşımına dayanmaktadır [34]. Düzenleme, yapay zekâ sistemlerini risk düzeyine göre sınıflandırarak yüksek riskli alanlara şeffaflık, insan denetimi ve hesap verebilirlik yükümlülükleri getirmektedir. Bu yaklaşım aynı zamanda Avrupa'nın teknolojik geride kalma riskini standart belirleyici güçle dengeleme stratejisinin bir parçasıdır.

Türkiye'nin yapay zekâ alanındaki yasal ve kurumsal çerçevesi gelişimini sürdürmektedir. Bununla birlikte son yıllarda önemli politika ve kapasite oluşturma adımları atılmıştır. 2021 yılında Cumhurbaşkanlığı Genelgesiyle yürürlüğe giren Ulusal Yapay Zekâ Stratejisi, 12. Kalkınma Planı doğrultusunda 2024-2025 döneminde güncellenmiş; yapay zekânın ekonomik ve toplumsal dönüşümdeki rolünü güçlendirmeye yönelik hedefler ortaya koymuştur [35]. Bu çerçevede özellikle Türkçe büyük dil modellerinin geliştirilmesi, yüksek başarılı hesaplamalı altyapılarına erişimin artırılması ve üretken yapay zekâ teknolojilerinin kamu hizmetlerine entegrasyonu öncelikli çalışma alanları arasında yer almıştır [36].

Bu hedefler doğrultusunda son dönemde somut ilerlemeler de kaydedilmiştir. TÜBİTAK BİLGEM koordinasyonunda geliştirilen Türkçe büyük dil modeli çalışmalarının kamu eri-

şimine açılması, Türkiye'nin yapay zekâ değer zincirinde yalnızca uygulama katmanında değil, temel model geliştirme kapasitesi bakımından da yetkinlik oluşturmaya yönelik çabalarının önemli göstergelerinden biri olarak değerlendirilebilir. Her ne kadar küresel ölçekteki öncü modellerle karşılaştırıldığında bu alandaki rekabet oldukça yoğun olsa da yerli temel model geliştirme girişimleri yapay zekâ alanındaki teknolojik kapasitenin ve dijital egemenlik hedeflerinin güçlendirilmesi açısından stratejik önem taşımaktadır.

13 Haziran 2026 tarihinde açıklanan Türkiye Yapay Zekâ Vizyonu ve 2026-2030 Eylem Planı ise bu yaklaşımı daha ileri bir aşamaya taşıyarak insan kaynağının geliştirilmesi, veri ve hesaplama altyapılarının güçlendirilmesi, yapay zekâ uygulamalarının yaygınlaştırılması, veri egemenliği ve dijital egemenlik kapasitesinin artırılması ile yapay zekâ yönetişiminin kurumsallaştırılması gibi stratejik öncelikleri politika gündeminin merkezine yerleştirmiştir. Özellikle sağlık, tarım, savunma ve elektronik ticaret başta olmak üzere kamu kurumlarında üretilen veri setlerinin Ulusal Veri Kütüphanesi aracılığıyla araştırmacıların, girişimlerin ve kamu kurumlarının kullanımına açılmasının hedeflenmesi dikkat çekici bir gelişmedir. Bu yaklaşım yalnızca yapay zekâ sistemlerinin geliştirilmesi için gerekli veri kaynaklarının çeşitlendirilmesine katkı sağlamakla kalmamakta, aynı zamanda veri egemenliğini koruyarak kontrollü veri paylaşımını mümkün kılan veri alanları (*data spaces*) ve düzenleyici deney alanları (*regulatory sandboxes*) gibi uluslararası uygulamalarla da uyum göstermektedir. Planın temel eksenleri kamuoyuyla paylaşılmış olmakla birlikte, uygulama mekanizmalarına ve hedeflere ilişkin ayrıntılı dokümanların yayımlanma süreci devam etmektedir.

Bu çerçeve, 18 Ağustos 2026 tarihli Resmî Gazete'de yayımlanan Cumhurbaşkanlığı Genelgesi ile birlikte resmî bir statü kazanmış ve Eylem Planı'nın mimarisi netleşmiştir. Plan, "Fark Et, İstifade Et, Üret ve Yönet" şeklinde tanımlanan dört temel eksen üzerine kurulmuş; her eksen altında dörder eylem olmak üzere toplam on altı öncelikli eylem etrafında yapılandırılmıştır. Eylemler; yapay zekâ ekosisteminin enerji, hesaplama donanımı, altyapı, modeller/veri ve uygulamalardan oluşan beş temel katmanının yanı sıra yetenek, finansman ve düzenleme alanlarını güçlendirmeye yönelik olarak tasarlanmıştır. Bu katmanlı yapı, salt bir hedef listesinin ötesinde, küresel yapay zekâ değer zincirinin bütününe kapsayan sistematik bir okuma sunması bakımından dikkat çekicidir.

Katmanların sıralanışı da stratejik açıdan anlamlıdır. Enerji ve hesaplama donanımı gibi en alttaki katmanlarda küresel değer zincirinin yapısı gereği belirleyici olan sınırlı sayıda aktörün varlığı, Türkiye'nin bu alanlarda gerçekçi manevra alanının model/veri ve uygulama katmanlarında yoğunlaştığına işaret etmektedir. Planın "sektörel temel modeller" ve kamu veri setlerinin açılması gibi önceliklere ağırlık vermesi, bu gerçekçi konumlandırmanın bir yansıması olarak değerlendirilebilir: Türkiye, en ileri düzey genel amaçlı modeller yarışında değil, veri avantajına sahip olduğu dikey alanlarda (sağlık, tarım, savunma, elektronik ticaret) bu avantajı yerli modellere dönüştürme stratejisini benimsemektedir. Nitekim ABD ile Çin arasındaki hesaplama gücü ve yarı iletken eksenli rekabetin ve DeepSeek örneğinde görüldüğü üzere algoritmik verimliliğin denklemi karmaşıktırdığı bir konjonktürde, bu yaklaşım Türkiye'nin sınırlı kaynaklarını en yüksek getiriyle değerlendirebileceği alanlara odaklanması anlamına gelmektedir.

Yasal düzenleme cephesinde ise süreç henüz tamamlanmamıştır. TBMM'ye ilk kez Haziran 2024'te sunulan Yapay Zekâ Kanun Teklifi'nin ardından Eylül, Kasım ve Aralık 2025'te farklı milletvekilleri tarafından yeni teklifler gündeme getirilmiştir [37]. Bu teklifler; yapay zekâ sistemlerinin tanımlanması, geliştirici ve işletmeci sorumluluklarının belirlenmesi, yüksek riskli uygulamalara yönelik denetim mekanizmalarının oluşturulması, deepfake içeriklerin etiketlenmesi ve çeşitli idari yaptırım mekanizmalarının düzenlenmesi gibi konuları kapsamaktadır. Ancak teklifler arasındaki yaklaşım farklılıkları ve kapsamlı bir çerçeve kanunun henüz yasalaşmamış olması, Türkiye'nin yapay zekâ alanındaki düzenleyici mimarisinin hâlen oluşum aşamasında olduğunu göstermektedir. Avrupa Birliği'nin AI Act düzenlemesinin Türkiye'deki politika ve mevzuat tartışmalarını önemli ölçüde etkilediği görülmekte; bu durum yapay zekâ yönetişimi alanında da Brüksel Etkisi'nin hissedildiğine işaret etmektedir.

Türkiye açısından temel gerilim ise devam etmektedir. Bir tarafta yerli yapay zekâ kapasitesini artırmaya, veri egemenliğini güçlendirmeye ve ulusal hesaplama altyapıları oluşturmaya yönelik güçlü bir politika iradesi bulunmaktadır. Diğer tarafta ise ileri düzey yapay zekâ modellerinin geliştirilmesi için gerekli olan yarı iletken teknolojileri, yüksek performanslı hesaplama altyapıları, temel modeller ve küresel veri ekosistemleri büyük ölçüde uluslararası teknoloji şirketlerinin kontrolündedir. Bu yapısal asimetri, Türkiye'nin yapay zekâ alanında gerçek anlamda stratejik özerklik kazanmasının önündeki temel engellerden birini oluşturmaktadır. Dolayısıyla son dönemde hız kazanan kurumsal ve stratejik girişimlere rağmen, Türkiye'nin yapay zekâ alanında daha yüksek düzeyde teknolojik bağımsızlık ve stratejik kapasite geliştirebilmesi; yalnızca düzenleyici çerçevenin tamamlanmasına değil, aynı zamanda hesaplama gücü, veri altyapısı ve temel model geliştirme yetkinliklerinin yerli ölçekte güçlendirilmesine de bağlıdır.

4.4 Dijital Platformlar ve Demokratik Süreçler

Dijital platformların güç yoğunlaşması, demokratik süreçler açısından da önemli tartışmalar yaratmaktadır. Özellikle sosyal medya platformları ve arama motorları, kamusal tartışmanın temel kanalları haline gelmiştir. Milyarlarca insan haber içeriklerine, siyasi tartışmalara ve toplumsal gelişmelere büyük ölçüde dijital platformlar aracılığıyla erişmektedir [38]. Büyük dijital platformlar artık yalnızca özel sektör aktörleri olarak değerlendirilememektedir. Arama motorları, sosyal medya ağları ve uygulama mağazaları fiilen kamusal iletişimin ve ekonomik faaliyetlerin temel erişim altyapıları haline gelmiştir.

Bu durum platformların ekonomik aktörler olmasının yanı sıra aynı zamanda siyasal aktörler haline gelmesine yol açmaktadır. Hangi içeriğin öne çıkarıldığı, hangi haberlerin daha görünür hale geldiği ve hangi hesapların erişiminin sınırlandırıldığı gibi kararlar, kamusal tartışmanın niteliğini doğrudan etkilemektedir [39].

Cambridge Analytica vakası, dijital platformların demokratik süreçler üzerindeki etkisini görünür hale getiren en önemli örneklerden biri olmuştur [40]. Milyonlarca kullanıcının kişisel verisinin siyasi hedefleme amacıyla kullanılması, veri ekonomisinin demokratik süreçlerle nasıl kesiştiğini açık biçimde göstermiştir.

Benzer şekilde yanlış bilgi, dezenformasyon ve algoritmik kutuplaşma tartışmaları da platformların toplumsal etkisini artırmaktadır. Algoritmaların kullanıcı etkileşimini artırmaya yönelik tasarımı, çoğu zaman daha sert, daha duygusal ve daha kutuplaştırıcı içeriklerin görünürlüğünü artırabilmektedir [41]. Bu durum yalnızca bireysel tercihleri değil; kamusal tartışma kültürünü de etkilemektedir.

Bu tartışmalar çerçevesinde “algoritmik çoğulculuk” yaklaşımı daha fazla önem kazanmaktadır. Demokratik toplumlarda bilgiye erişimin tek bir algoritmik sistem üzerinden şekillenmesi, kamusal tartışmanın çeşitliliği açısından risk yaratabilmektedir. Kullanıcıların farklı bilgi sıralama ve öneri sistemleri arasında tercih yapabilmesi, dijital kamusal alanın çoğulcu yapısının korunması açısından önemli görülmektedir.

Bu nedenle son yıllarda “algoritmik şeffaflık” ve “platform hesap verebilirliği” kavramları daha fazla önem kazanmaktadır. Özellikle Avrupa Birliği’nin Dijital Hizmetler Yasası (DSA) ile birlikte büyük platformlara yönelik şeffaflık yükümlülükleri artırılmıştır [42]. Amaç, dijital platformların kamusal etkisini daha görünür ve denetlenebilir hale getirmektir.

4.5 Dijital Egemenlik Tartışmalarında Türkiye’nin Konumu

Türkiye, dijital dönüşüm sürecini yoğun biçimde yaşayan ülkeler arasında yer almaktadır. Kamu hizmetlerinin dijitalleşmesi, e-Devlet altyapısının gelişmesi ve mobil internet kullanımının yaygınlaşması, dijital ekonominin hızlı biçimde büyümesini sağlamıştır. Bununla birlikte bu büyümenin önemli bölümü, yabancı platformların altyapısı üzerinde gerçekleşmektedir. Dijital ekonominin temel erişim noktaları olan arama motorları, sosyal medya platformları, mobil işletim sistemleri, uygulama mağazaları, bulut bilişim hizmetleri ve dijital reklam altyapıları büyük ölçüde yabancı şirketlerin kontrolündedir [43]. Bu yapı, dijital ekonominin büyümesiyle birlikte dışa bağımlılık ilişkilerinin de paralel biçimde derinleştiği bir tablo ortaya koymaktadır.

Bu bağımlılık ilişkisi yalnızca ekonomik değil; stratejik bir kırılganlık olarak değerlendirilmelidir. Daha önce incelenen ülke deneyimleri, **özellikle ABD’nin ve Çin’in** teknolojiyi ve bünyelerindeki şirketleri egemenlik alanlarını genişletmek için bilinçli biçimde kullandığını göstermektedir. CLOUD Act kapsamında yabancı bulut altyapılarına emanet edilen verilere ABD makamlarının erişebildiği bir hukuki çerçevede, Türk kamu kurumlarının ve özel sektörün söz konusu altyapılara olan bağımlılığı doğrudan bir egemenlik sorunu haline gelmektedir. Benzer biçimde Çin kökenli altyapı ve yazılımların Ulusal İstihbarat Kanunu ve Askeri-Sivil Füzyon politikası çerçevesinde taşıdığı riskler de Türkiye açısından ciddi değerlendirme gerektirmektedir.

Bulut altyapısı ve e-Devlet entegrasyonu bu bağlamda birincil öncelik taşımaktadır. Türkiye, kamu kurumlarının verilerini ticari bulut altyapılarına taşıma sürecini başlatmıştır. Hazırlanan Kamu Bulut Bilişim Stratejisi, kritik verilerin yurt içinde barındırılmasını temel kural olarak belirlemiştir, öte yandan stratejide yurt dışı altyapılardan hizmet alımının kamu kurumlarının inisiyatifine bırakılabileceği bir esneklik kapısının açık bırakıldığı görülmektedir [44]. Bu belirsizlik, kritik kamu verilerinin hangi koşullarda yabancı altyapılara taşınabileceğine ilişkin denetim eksikliğini işaret etmektedir. e-Devlet hizmetlerinin dijital

altyapıya olan bağımlılığı göz önünde bulundurulduğunda, bu altyapının kimin tarafından işletildiği sorusu teknik bir tercihten öte, doğrudan kamusal düzen ve egemenlik meselesi haline gelmektedir.

Dijital reklam pazarı ise görünürde ticari bir alan olarak değerlendirilse de toplumsal boyutuyla çok daha derin bir öneme sahiptir. Türkiye'nin dijital reklam ekosistemi son yıllarda istikrarlı biçimde büyümekte; dijital mecraların toplam medya yatırımları içindeki payı her yıl artmaktadır [45]. Reklamcılar Derneği, IAB Türkiye ve diğer sektör kuruluşları adına Deloitte tarafından hazırlanan araştırmalar, 2024 yılında Türkiye'deki toplam medya ve reklam yatırımlarının 253,6 milyar TL'ye ulaştığını; medya yatırımlarının yüzde 74,2'sinin dijital mecraya yöneldiğini ve Türkiye'nin yüzde 39,4'lük büyüme oranıyla en fazla büyüyen ülkeler arasına girdiğini ortaya koymaktadır [46]. Bu büyümeden elde edilen gelirin büyük bölümü Google ve Meta gibi küresel platformlara akmaktadır. Buradaki asıl sorun yalnızca ekonomik değildir. Dijital reklam altyapısını elinde tutan platformlar, hangi içeriğin kime, ne zaman ve nasıl gösterileceğini belirlemektedir. Hedefli reklam mekanizmaları, kullanıcıların ilgi alanlarını, siyasi eğilimlerini ve tüketim alışkanlıklarını profillemekte; bu profiller aynı zamanda davranışsal yönlendirme ve toplumsal rıza üretiminin altyapısını oluşturmaktadır. Dijital reklamın bu boyutu, yalnızca ticari bir pazar dinamiği değil; toplumsal gündem ve kültürel değişim üzerinde sessiz ama kalıcı bir etki mekanizmasıdır.

Kritik altyapıların korunmasında yabancı sistem bağımlılığı ise bu tablonun en hassas boyutunu oluşturmaktadır. Enerji şebekeleri, bankacılık sistemleri, sağlık altyapıları, ulaşım ağları ve kamu iletişim sistemleri büyük ölçüde yabancı üreticilerin donanım ve yazılımlarına dayanmaktadır. Bu durum, soyut bir güvenlik açığının ötesinde somut bir stratejik risk barındırmaktadır: Kritik altyapıları koruyan sistemlerin yabancı kökenli olması, olası bir uluslararası kriz veya çatışma ortamında o sistemlerin güvenilirliğine ilişkin köklü bir belirsizlik yaratmaktadır. Nitekim 2024 yılında MERNİS ve PolNet sistemlerinde yaşanan veri sızıntıları ile TEDAŞ'ın 2022 yılında maruz kaldığı siber saldırı, bu kırılganlıkların teorik değil; fiilen gerçekleşmiş riskler olduğunu somut biçimde ortaya koymaktadır [47].

Türkiye bu gerçekliğe yanıt üretme yolunda, 19 Mart 2025'te yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, Türkiye'de siber güvenlik alanında ilk kapsamlı yasal çerçeveyi oluşturmuştur [48]. Kanun; elektronik haberleşme, enerji, su yönetimi, ulaştırma, sağlık ile bankacılık ve finans sektörlerini kritik altyapı kapsamında tanımlamakta, Siber Güvenlik Başkanlığı'na bu alanlarda geniş denetim ve müdahale yetkileri tanımaktadır. Özellikle dikkat çekici olan, 2025 yılı itibarıyla stratejik sektörlerde siber savunma envanterindeki dışa bağımlılığı azaltmak amacıyla Yerli İkame Zorunluluğu'nun yürürlüğe girmiş olmasıdır [49]. Bu adım, salt güvenlik tedbirinin ötesinde dijital egemenlik tartışmasının somut bir politika aracına dönüşmeye başladığının göstergesidir.

Dijital egemenlik tartışmaları son dönemde yapay zekâ politikaları üzerinden de yeni bir boyut kazanmıştır. 2026 yılında açıklanan Türkiye Yapay Zekâ Vizyonu ve 2026-2030 Eylem Planı, yapay zekâyı yalnızca ekonomik büyüme veya teknolojik dönüşüm aracı olarak değil, aynı zamanda stratejik kapasite ve rekabet unsuru olarak konumlandırmaktadır. Özellikle kamu verilerinin kontrollü biçimde araştırma ve inovasyon ekosistemine açılmasına yönelik yaklaşım, verinin yalnızca korunması gereken bir unsur değil, ulusal kapasite

üretiminin temel girdilerinden biri olarak değerlendirilmeye başlandığını göstermektedir. Bu yönüyle plan, Türkiye’de dijital egemenlik tartışmalarının siber güvenlik ve veri koruma ekseninden çıkarak veri, yapay zekâ ve teknolojik yetkinlik boyutlarını da içeren daha kapsamlı bir çerçeveye evrilmekte olduğuna işaret etmektedir.

Eylem Planı’nın resmî yayımıyla birlikte bu çerçeve, ölçülebilir hedefler ve tanımlı bir yönetim mimarisiyle de desteklenmiştir. Planda; yapay zekâ okuryazarlığında ilk on iki ayda en az 1,5 milyon, yirmi dört ay sonunda toplam 5 milyon vatandaşa ulaşılması, seksen bir ilde düzenli atölyeler gerçekleştirilmesi, on bin ileri düzey uzman ile yüz bin uygulama profesyonelinin yetiştirilmesi ve en az iki bin kamu veri setinin Ulusal Veri Kütüphanesi üzerinden makine okunabilir biçimde erişime açılması gibi somut hedefler tanımlanmıştır. Bu hedeflerin, ana sorumlu kurumların ve performans göstergelerinin eylem bazında belirlendiği bir yapıda sunulması dikkat çekicidir. Uygulamanın koordinasyonu; en üst karar ve eşgüdüm organı olarak Ulusal Yapay Zekâ Kurulu, uygulama takibinden sorumlu Program Ofisi, etik rehberlik işlevini üstlenen Ulusal Yapay Zekâ Etik Kurulu ve tüm eylemlerin hedef-bütçe-zaman uyumunu kamuya açık biçimde izleyecek Ulusal Yapay Zekâ İlerleme ve Şeffaflık Portalı aracılığıyla yürütülecektir. İzleme ve hesap verebilirliği merkeze alan bu yapı, Türkiye’de stratejik belgelerin uygulama boyutunun güçlendirilmesi bakımından olumlu bir yönelime işaret etmektedir. Böylece plan, dijital egemenlik tartışmalarını siber güvenlik ve veri koruma ekseninden çıkararak; veri, hesaplama kapasitesi, yerli model geliştirme ve yönetim boyutlarını da kapsayan bütüncül bir politika çerçevesine taşımaktadır.

Bununla birlikte Türkiye’nin bu alanda karşı karşıya olduğu temel sorunlardan biri, düzenleyici kapasite ile ekonomik bağımlılık arasındaki yapısal dengesizliktir. Bir yanda dijital reklam gelirlerinin büyük bölümü yabancı platformlara akmakta, kamu bulut geçişi tartışmalı bir denetim çerçevesinde ilerlemekte ve kritik altyapılardaki yabancı yazılım bağımlılığı kısa sürede çözüme kavuşturulamamaktadır. Öte yanda yeni kurumsal yapılar, yasal çerçeveler ve stratejik belgeler bu bağımlılıkların farkındalığının arttığını ve politika gündemine girdiğini göstermektedir. Türkiye açısından temel mesele, dijitalleşmeye karşı korumacı bir yaklaşım geliştirmek değil; stratejik bağımlılıkları azaltacak, düzenleyici kapasiteyi güçlendirecek ve kritik altyapılar üzerinde daha yüksek denetim sağlayacak bir politika çerçevesi oluşturmaktır.

5. Türkiye’de Dijital Bağımlılık ve Sektörel Analiz

5.1 Türkiye’de Dijital Ekonominin Yapısı

Türkiye’de dijital ekonominin büyümesi son on yıl içinde hız kazanmıştır. We Are Social ve Meltwater’ın Dijital 2025 Türkiye Raporu’na göre ülkedeki aktif internet kullanıcısı sayısı 77,3 milyona ulaşmış; bu rakam toplam nüfusun yüzde 88,3’üne karşılık gelmektedir [50]. Mobil internet kullanımının yaygınlaşması, elektronik ticaret hacmindeki artış, dijital ödeme sistemlerinin gelişmesi ve kamu hizmetlerinin çevrim içi platformlara taşınması, dijital teknolojileri ekonomik yaşamın merkezine yerleştirmiştir. Özellikle pandemi sonrasında dijital platformlar yalnızca iletişim ve eğlence alanında değil; ticaret, eğitim, finans ve kamu hizmetleri bakımından da temel altyapılar haline gelmiştir [2].

Bununla birlikte Türkiye’de dijital ekonominin temel erişim noktalarının önemli bölümü küresel teknoloji şirketlerinin kontrolü altındadır. Arama motoru hizmetleri, sosyal medya platformları, mobil işletim sistemleri, uygulama mağazaları, bulut bilişim hizmetleri ve dijital reklam altyapıları büyük ölçüde yabancı şirketler tarafından işletilmektedir [43]. Bu durum, dijital ekonominin büyümesiyle birlikte dışa bağımlılık ilişkilerinin de paralel biçimde derinleştiği bir tablo ortaya koymaktadır.

Türkiye’nin dijital teknoloji sektöründeki büyüme aynı zamanda yabancı sermayenin artan ilgisini de beraberinde getirmektedir. 2025 yılı itibarıyla Türkiye’nin önde gelen teknoloji platformlarından N11’in Abu Dabi merkezli DMSF Holding’e devredilmesi ve Trendyol GO’nun ABD’li Uber tarafından satın alınması, bu trendin sürdüğünü açıkça ortaya koymaktadır [51]. Bu gelişmeler, dijital ekonominin büyümesinin stratejik kontrolün giderek daha fazla yabancı aktörlerin eline geçmesiyle eş zamanlı ilerlediğini göstermektedir.

Platform yoğunlaşması, reklam maliyetleri ve uygulama mağazası komisyonları üzerinden yerli işletmeler açısından önemli bir rekabetçi dezavantaj yaratmaktadır. Apple App Store ve Google Play Store, mobil uygulamaların kullanıcılara ulaşabilmesi açısından fiili erişim noktaları haline gelmiştir. Platform komisyonları, ödeme altyapısı kuralları ve uygulama mağazası politikaları, yerli yazılım şirketlerinin ekonomik faaliyetlerini doğrudan şekillendirmekte; ölçeklenme kapasitelerini sınırlandırmaktadır [52].

Türkiye’nin dijital ekonomisi büyümeye devam ederken bu büyümenin hangi altyapılar üzerinde gerçekleştiği ve bu altyapıların kimin kontrolünde olduğu sorusu giderek daha kritik bir boyut kazanmaktadır.

5.2 Rekabet Hukuku ve Dijital Piyasalar

Dijital platformların ekonomik gücü, rekabet hukuku alanında yeni tartışmaları beraberinde getirmiştir. Geleneksel rekabet hukuku araçları büyük ölçüde fiyat temelli analizlere dayanırken, dijital piyasalarda veri yoğunlaşması, ağ etkileri ve platform bağımlılığı gibi unsurlar daha belirleyici hale gelmiştir [53]. Bu nedenle birçok ülkede dijital platformlara yönelik yeni düzenleyici yaklaşımlar geliştirilmektedir [54].

Türkiye’de Rekabet Kurumu son yıllarda dijital platformlara ilişkin soruşturmasını ve sektör incelemelerini artırmıştır. Özellikle Google hakkında yürütülen soruşturmalar arama motorları, reklam teknolojileri ve Android ekosistemi üzerindeki yoğunlaşmaya odaklanmıştır. Bu süreçler Avrupa Birliği rekabet hukuku uygulamalarıyla paralel biçimde gelişmekte; Türkiye’nin AB’nin Dijital Piyasalar Yasası yaklaşımını yakından izlediği görülmektedir [55].

Bununla birlikte dijital platformların ekonomik yapısı klasik rekabet hukuku müdahalelerini zorlaştırmaktadır. Ağ etkileri ve veri yoğunlaşması nedeniyle piyasaya yeni giriş yapan aktörlerin rekabetçi ölçekte büyümesi son derece güç hale gelmektedir. Ayrıca dijital hizmetlerin çoğu kullanıcılar açısından ücretsiz sunulduğundan fiyat artışı merkezli klasik zarar analizleri yetersiz kalmaktadır [9].

Bu nedenle Avrupa Birliği tarafından kabul edilen Dijital Piyasalar Yasası belirli platformları “eşik bekçisi” olarak tanımlamakta ve bu şirketlere özel yükümlülükler getirmek-

tedir [11]. Türkiye açısından benzer düzenleyici araçların hangi ölçüde ve hangi kurumsal kapasiteyle uygulanabileceği, önümüzdeki dönemin temel tartışma gündemlerinden birini oluşturmaktadır.

5.3 Veri Koruma ve Düzenleyici Kurumlar

Türkiye’de kişisel verilerin korunmasına ilişkin temel çerçeve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile oluşturulmuştur [56]. Kanun veri işleme süreçlerine ilişkin temel ilkeleri belirlemekte ve veri sorumlularına çeşitli yükümlülükler getirmektedir. Bununla birlikte dijital platform ekonomisinin ölçeği ve karmaşıklığı arttıkça veri koruma alanındaki gerilimler de derinleşmektedir.

Özellikle büyük teknoloji şirketlerinin kullanıcı verilerini küresel ölçekte işlemesi, veri transferi ve veri egemenliği tartışmalarını daha kritik bir noktaya taşımıştır. Kullanıcı davranışlarının yüksek yoğunluklu veri analizleri aracılığıyla ekonomik değere dönüştürülmesi yalnızca bir mahremiyet meselesi değil; aynı zamanda ekonomik güç yoğunlaşması ve stratejik bağımlılık sorunu olarak değerlendirilmelidir [57].

Türkiye’de siber güvenlik alanındaki düzenleyici çerçeve 2025 yılında köklü biçimde güçlendirilmiştir. 19 Mart 2025’te yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu’nun verdiği yetkiyle toplanan Siber Güvenlik Kurulu, elektronik haberleşme, enerji, su yönetimi, ulaştırma, sağlık ile bankacılık ve finans sektörlerini de kapsayan 14 sektörü kritik altyapı kapsamında tanımlamakta; Siber Güvenlik Başkanlığı’na bu alanlarda geniş denetim ve müdahale yetkileri tanımaktadır [48]. Bu yasal çerçeve, Türkiye’de siber güvenlik alanındaki kurumsal kapasitenin önemli bir sıçrama yaptığıının göstergesidir.

Bununla birlikte Türkiye’de Rekabet Kurumu, Bilgi Teknolojileri ve İletişim Kurumu, Kişisel Verileri Koruma Kurumu ve Siber Güvenlik Başkanlığı dijital platformlarla ilişkili alanlarda birbirinden farklı yetkilere sahip olup dijital platform ekonomisinin çok katmanlı yapısı bu kurumlar arasında daha güçlü koordinasyon ihtiyacını zorunlu kılmaktadır. Avrupa Birliği’nin veri koruma, rekabet hukuku ve içerik düzenlemelerini giderek daha bütünleşik bir çerçevede ele aldığı düşünüldüğünde, Türkiye açısından da benzer birçok disiplinli yönetim yaklaşımının geliştirilmesi kaçınılmaz görünmektedir [58].

5.4 Stratejik Özerklik ve Politika Seçenekleri

Türkiye’nin dijital bağımlılık haritası değerlendirildiğinde üç kritik eksen öne çıkmaktadır: telekomünikasyon ve ağ altyapısı, bulut bilişim ve veri işleme, kritik sektörlerin siber korunması. Bu üç eksenin her biri farklı düzeylerde stratejik kırılganlık barındırmaktadır.

Telekomünikasyon altyapısı açısından Türkiye, mobil şebeke ekipmanları başta olmak üzere yabancı üreticilere önemli ölçüde bağımlı görünmektedir. Türk Telekom ve Huawei’nin akıllı şehircilik ve 5G-Advanced altyapıları alanında sürdürdüğü iş birlikleri, Çin kökenli altyapı teknolojisinin Türkiye’nin telekomünikasyon ekosistemine ne ölçüde entegre olduğunu gözler önüne sermektedir [59]. Daha önce ayrıntılı biçimde incelenen Çin’in Ulusal İstihbarat Kanunu ve Askeri-Sivil Füzyon politikası çerçevesinde bu entegrasyon düzeyi yalnızca ticari bir tercih olarak değil; potansiyel bir güvenlik değişkeni olarak da değerlendirilmelidir [27, 28].

Bulut altyapısı cephesinde ise tablo benzer bir yapısal gerilimi yansıtmaktadır. Küresel bulut pazarı Microsoft Azure, Amazon Web Services ve Google Cloud'un fiili oligopolünde şekillenmiş durumdadır. Bu üç sağlayıcının yaşadığı büyük kesintilerin, Microsoft Azure'a hizmet veren CrowdStrike çöküşü ve Google Cloud'da yaşanan yanlış yapılandırma krizi dahil, dünya çapındaki operasyonları felce uğrattığı görülmüş; uzmanlar küresel internetin bu kadar az sayıda sağlayıcıya bağımlı olmasının ciddi riskler oluşturduğunu açıkça ortaya koymuştur [60]. Türkiye'nin kamu kurumlarının ve özel sektörünün bu altyapılara olan bağımlılığı, olası bir kesinti veya jeopolitik kriz senaryosunda kamusal hizmetlerin kesintisiz sürdürülmesi açısından doğrudan bir kırılganlık noktası oluşturmaktadır [44].

Kritik sektörlerin siber korunması ise en hassas boyutu oluşturmaktadır. Enerji şebekeleri, bankacılık sistemleri, sağlık altyapıları, ulaşım ağları ve kamu iletişim sistemlerinin büyük bölümü yabancı üreticilerin donanım ve yazılımlarına dayanmaktadır. Kritik altyapıları koruyan sistemlerin yabancı kökenli olması, olası bir uluslararası kriz veya çatışma ortamında bu sistemlerin güvenilirliğine ilişkin köklü bir belirsizlik doğurmaktadır [47, 48].

2025 yılı itibarıyla stratejik sektörlerde siber savunma envanterindeki dışa bağımlılığı azaltmak amacıyla Yerli İkame Zorunluluğu yürürlüğe girmiştir [49]. Bunun güncel örnekleri T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB) koordinasyonunda ve büyük savunma sanayii şirketleri iş birliğinde hayata geçirilmektedir [61]. Bu adımlar, salt güvenlik tedbiri olmanın ötesinde dijital egemenlik tartışmasının somut bir politika çıktısına dönüşmeye başladığının önemli bir göstergesidir.

Bununla birlikte stratejik özerklik yolculuğu uzun vadeli bir süreçtir. Tam anlamıyla teknolojik bağımsızlık kısa vadede gerçekçi bir hedef olarak görülmemekle birlikte kritik dijital altyapılar üzerindeki bağımlılıkların azaltılması ve düzenleyici kapasitenin güçlendirilmesi mümkündür [62]. Bu çerçevede öncelik sıralaması belirgin biçimde ortaya çıkmaktadır: kamu kurumlarının dijital altyapı bağımlılıklarının sistematik biçimde haritalanması; yerli bulut bilişim, siber güvenlik ve yapay zekâ kapasitesinin stratejik sektörlerde artırılması; düzenleyici kurumlar arasındaki koordinasyonun güçlendirilmesi ve dijital piyasalara yönelik proaktif düzenleme araçlarının geliştirilmesi [63].

Türkiye açısından temel mesele, dijitalleşmeye karşı korumacı bir yaklaşım benimsemek değil; stratejik bağımlılıkları azaltacak, düzenleyici kapasiteyi güçlendirecek ve kritik altyapılar üzerinde daha yüksek denetim sağlayacak bir politika çerçevesi oluşturmaktır. Dijital egemenlik, küresel dijital ekonomiden kopuş değil; bu ekonomiyle daha eşit koşullarda ve daha güçlü karar alma kapasitesiyle bütünleşmenin adıdır.

18 Ağustos 2026'da yürürlüğe giren Türkiye Yapay Zekâ Eylem Planı (2026-2030), bu stratejik özerklik perspektifiyle örtüşen somut araçlar sunmaktadır. Planın öngördüğü yerli ve sektörel temel model geliştirme, hesaplama kapasitesinin araştırmacı ve girişimlerin doğrudan erişimine açılması ile kamu veri setlerinin kontrollü paylaşımı; bu bölümde ortaya konulan bağımlılığı yönetilebilir kılma yaklaşımının uygulama zeminini genişletmektedir. Özellikle planın enerji ve hesaplama donanımı katmanlarını ekosistemin temeline yerleştirmesi, yapay zekâ kapasitesinin yalnızca yazılım ve model geliştirmeye değil; veri merkezi, bulut ve işlem gücü altyapısıyla birlikte ele alınması gereken bütünleşik bir me-

sele olduğu yönündeki tespitle uyumludur. Bu araçların stratejik özerkliğe katkısı ise nihai olarak, tanımlanan hedeflerin sürdürülebilir kurumsal kapasiteye ve istikrarlı finansman mekanizmalarına dönüştürülebilmesine bağlı olacaktır.

Bu çerçevede planın öngördüğü finansman mimarisi, stratejik özerklik tartışması açısından özellikle dikkate değerdir. Plan; kamu kaynakları ile özel sektör yatırımlarının ortak hedefler etrafında harekete geçirilmesiyle, uygulama döneminde bir trilyon lirayı aşan bir ekonomik değer üretilmesini öngörmektedir. Bu değer, salt bir büyüme rakamı olmanın ötesinde; teknolojik bağımsızlık, kamu hizmetlerinin niteliği ve üretim yapısının dönüşümü gibi boyutlarla birlikte tanımlanmaktadır. Finansmanın kurumsal omurgasını ise temel araştırmadan girişim ölçeklenmesine uzanan bir merdiven oluşturmaktadır: erken aşama ve temel araştırmayı destekleyecek Ulusal Yapay Zekâ Araştırma Fonu ile olgunlaşan girişimlerin ölçeklenmesini hızlandıracak Yapay Zekâ Büyüme Fonu. Kamu kaynağının her bir birimine karşılık en az iki birim özel sermayenin mobilize edilmesinin hedeflenmesi, bu yaklaşımın kamu yatırımını piyasayı dışlayan değil; tetikleyen bir kaldıraç olarak kurgulamayı amaçladığını göstermektedir. Bu mimarinin stratejik özerkliğe katkısı, nihai olarak fonların sürdürülebilir biçimde kaynaklandırılması ve yerli girişim ekosisteminin bu kaynakları ölçeklenebilir teknolojilere dönüştürebilme kapasitesine bağlı olacaktır.

6. Dijital Yönetişimin Küresel Anatomisi: AB Modeli ve Ötesi

6.1 Avrupa Birliği'nin Dijital Düzenleme Modeli

Avrupa Birliği son yıllarda dijital platformların ekonomik ve toplumsal etkilerine yönelik en kapsamlı düzenleyici çerçeveyi oluşturan aktörlerden biri haline gelmiştir. Özellikle rekabet hukuku, veri koruma, içerik denetimi ve yapay zekâ alanlarında geliştirilen yeni düzenlemeler, küresel teknoloji şirketlerinin faaliyetlerini doğrudan etkileyen sonuçlar doğurmaktadır [64].

Yine son yıllarda Avrupa Birliği içerisinde “EuroStack” yaklaşımı daha görünür hale gelmiştir. Bu yaklaşım, yarı iletkenlerden bulut altyapılarına, yapay zekâ modellerinden veri katmanlarına kadar uzanan yedi katmanlı bir dijital egemenlik mimarisi oluşturmaya hedeflemektedir. Avrupa Birliği'nin özellikle bulut altyapıları, yarı iletkenler ve yapay zekâ alanlarında yüksek dış bağımlılık düzeyi, stratejik özerklik tartışmalarını hızlandırmıştır.

Avrupa Birliği'nin yaklaşımı büyük ölçüde “dijital anayasacılık” olarak tanımlanan bir çerçeveye dayanmaktadır [58]. Bu yaklaşım, dijital platformların yalnızca piyasa aktörleri olarak değil; kamusal alan üzerinde etkili altyapılar olarak değerlendirilmesi gerektiği varsayımından hareket etmektedir. Böylece temel hakların korunması, rekabetin sürdürülmesi ve demokratik süreçlerin güvence altına alınması, dijital düzenlemelerin merkezine yerleşmektedir [65].

Bu yaklaşımın en önemli örneklerinden biri Dijital Piyasalar Yasası'dır (DMA). Avrupa Birliği, belirli ölçeğin üzerindeki platformları “kapı bekçisi” olarak tanımlayarak bu şirketlere özel yükümlülükler getirmiştir [11]. Amaç, platformların piyasa gücünü kullanarak rekabeti dışlayıcı davranışlarda bulunmasını engellemektir.

DMA kapsamında getirilen yükümlülükler arasında veri taşınabilirliği, birlikte çalışabilirlik, kendi hizmetlerini öne çıkarmama ve alternatif uygulama mağazalarına izin verilme-

si gibi kurallar yer almaktadır. Bu düzenlemeler, dijital piyasalardaki yapısal yoğunlaşmayı azaltmaya yönelik müdahaleler olarak değerlendirilmektedir [54].

Avrupa Birliği'nin ikinci önemli düzenleme alanı Dijital Hizmetler Yasası'dır (DSA). DSA, özellikle içerik denetimi, algoritmik şeffaflık ve platform hesap verebilirliği konularına odaklanmaktadır [42]. Büyük platformların risk değerlendirmesi yapması, içerik moderasyonu süreçlerine ilişkin şeffaflık sağlaması ve araştırmacılarla veri paylaşması gibi yükümlülükler bu yaklaşımın temel parçalarıdır [39].

Bu düzenlemeler, Avrupa Birliği'nin dijital alanı yalnızca ekonomik rekabet perspektifiyle değil; demokratik yönetim ve temel haklar ekseninde değerlendirdiğini göstermektedir.

6.2 Veriyi Yönetmek ve GDPR Yaklaşımı

Avrupa Birliği'nin dijital düzenleme alanındaki en etkili araçlarından biri Genel Veri Koruma Tüzüğü'dür (GDPR). 2018 yılında yürürlüğe giren düzenleme, kişisel verilerin işlenmesine ilişkin kapsamlı kurallar getirmiştir [66]. GDPR yalnızca Avrupa Birliği sınırları içinde faaliyet gösteren şirketleri değil; Avrupa Birliği vatandaşlarının verilerini işleyen küresel şirketleri de kapsamaktadır.

GDPR'nin en önemli özelliklerinden biri, veri koruma yaklaşımını temel hak perspektifiyle ilişkilendirmesidir. Kişisel verilerin korunması yalnızca teknik güvenlik meselesi olarak değil; bireyin özel yaşam hakkının bir parçası olarak değerlendirilmektedir [67].

GDPR kapsamında kullanıcıların açık rızası, veri taşınabilirliği hakkı, unutulma hakkı ve veri işleme süreçlerine ilişkin şeffaflık yükümlülükleri düzenlenmiştir. Ayrıca veri minimizasyonu, amaçla sınırlılık ve hesap verebilirlik ilkeleri, veri işleme faaliyetlerinin temel çerçevesini oluşturmaktadır [66]. Düzenleme, şirketlerin kullanıcı verilerini sınırsız biçimde toplamasını ve işlemesini engellemeyi; veri işleme faaliyetlerini belirli hukuki ve etik sınırlar içine yerleştirmeyi amaçlamaktadır.

GDPR'nin dikkat çekici yönlerinden biri, yalnızca bireysel mahremiyeti korumaya yönelik bir düzenleme olmamasıdır. Düzenleme aynı zamanda dijital platformların ekonomik gücünü sınırlandırmaya yönelik dolaylı etkiler de doğurmaktadır. Çünkü veri birikimi, platform ekonomisinin temel rekabet avantajlarından biridir. Kullanıcı verilerine erişimin ve bu verilerin işleme biçiminin düzenlenmesi, platformların ekonomik faaliyetlerini doğrudan etkilemektedir. Bu nedenle veri koruma hukuku ile rekabet hukuku arasındaki ilişki giderek daha görünür hale gelmektedir [57].

Avrupa Birliği Adalet Divanı'nın çeşitli kararları da bu yaklaşımı güçlendirmiştir. Özellikle "Google Spain" kararıyla birlikte unutulma hakkının tanınması, dijital platformların veri işleme faaliyetlerinin temel haklar perspektifiyle denetlenebileceğini göstermiştir [68]. Benzer biçimde Schrems kararları, Avrupa vatandaşlarının verilerinin Amerika Birleşik Devletleri'ne aktarılması konusunda daha sıkı standartlar geliştirilmesine yol açmıştır [30]. Böylece veri koruma tartışmaları yalnızca teknik güvenlik meselesi olmaktan çıkmış; uluslararası veri akışları, egemenlik ve temel haklar ekseninde değerlendirilen siyasi bir alan haline gelmiştir.

GDPR'nin küresel etkisi Avrupa Birliği sınırlarının ötesine geçmiştir. Birçok uluslararası şirket, faaliyetlerini Avrupa Birliği standartlarına göre yeniden düzenlemek zorunda kalmıştır. Bunun temel nedeni, Avrupa Birliği'nin büyük ekonomik pazar gücüyle bağlantılıdır. Küresel teknoloji şirketleri Avrupa pazarına erişimlerini sürdürebilmek için veri işleme politikalarını GDPR ile uyumlu hale getirmektedir. Akademik literatürde bu durum çoğu zaman "Brüksel Etkisi" kavramı çerçevesinde açıklanmaktadır [29]. Avrupa Birliği, ekonomik büyüklüğü sayesinde geliştirdiği düzenleme standartlarını filen küresel normlara dönüştürebilmektedir.

Veri koruma alanındaki bu yaklaşım, dijital egemenlik tartışmaları açısından da önemli sonuçlar doğurmaktadır. Avrupa Birliği'nin yaklaşımı, veriyi yalnızca ekonomik bir kaynak olarak değil; aynı zamanda demokratik toplum düzeniyle bağlantılı stratejik bir unsur olarak değerlendirmektedir [25]. Bu nedenle veri işleme süreçleri üzerinde kamusal denetimin artırılması, dijital egemenlik politikalarının temel araçlarından biri haline gelmiştir.

Türkiye açısından bakıldığında, 6698 sayılı Kişisel Verilerin Korunması Kanunu önemli bir başlangıç çerçevesi oluşturmuştur [56]. Bununla birlikte Avrupa Birliği'ndeki düzenleyici yaklaşım ile Türkiye'deki uygulama kapasitesi arasında belirgin farklar bulunmaktadır. Özellikle sınır ötesi veri aktarımı, platform denetimi ve büyük teknoloji şirketlerinin veri işleme faaliyetlerine ilişkin denetim kapasitesinin geliştirilmesi, önümüzdeki dönemin temel düzenleyici tartışma alanları arasında yer almaktadır.

Türkiye'de veri koruma rejiminin karşı karşıya olduğu temel sorunlardan biri, dijital platform ekonomisinin ölçeği ile mevcut denetim kapasitesi arasındaki dengesizliktir. Küresel teknoloji şirketleri çok katmanlı veri işleme modelleri, sınır aşan altyapılar ve karmaşık sözleşme ilişkileri üzerinden faaliyet göstermektedir. Buna karşılık ulusal düzenleyici kurumların teknik uzmanlık, insan kaynağı ve uluslararası koordinasyon kapasitesi çoğu zaman sınırlı kalmaktadır. Bu durum, veri koruma hukukunun yalnızca normatif düzeyde güçlü olmasının yeterli olmadığını; etkili uygulama kapasitesinin de en az hukuki çerçeve kadar önemli olduğunu göstermektedir.

Özellikle yapay zekâ sistemlerinin gelişmesiyle birlikte veri koruma tartışmaları yeni bir boyut kazanmıştır. Büyük dil modellerinin eğitimi için kullanılan veri setlerinin kapsamı, kişisel verilerin anonimleştirilmesi, telif hakkı sorunları ve otomatik karar alma mekanizmaları, klasik veri koruma yaklaşımlarını zorlayan alanlar haline gelmiştir [69]. Yapay zekâ sistemlerinin yüksek miktarda veriyle beslenmesi, veri ekonomisinin ölçeğini daha da büyütmemekte; bu durum platformların ekonomik ve teknolojik gücünü pekiştirmektedir [43].

Bu nedenle Avrupa Birliği'nde veri koruma, rekabet hukuku ve yapay zekâ düzenlemeleri giderek daha bütünleşik bir çerçevede ele alınmaktadır. Dijital platformların ekonomik gücü ile veri yoğunlaşması arasındaki ilişki daha görünür hale geldikçe, farklı düzenleme alanları arasındaki sınırlar da zayıflamaktadır. Rekabet hukuku artık yalnızca fiyat artışlarıyla değil; veri erişimi, algoritmik ayrımcılık ve platform bağımlılığı gibi unsurlarla da ilgilenebilmektedir [54].

Türkiye açısından bakıldığında da benzer bir bütüncül yaklaşım ihtiyacı ortaya çıkmak-

tadır. Dijital platformların etkisi yalnızca tek bir düzenleme alanı üzerinden yönetilebilecek ölçekte değildir. Rekabet hukuku, veri koruma hukuku, tüketici hukuku, siber güvenlik düzenlemeleri ve içerik denetimi mekanizmaları giderek daha fazla kesişmektedir. Bu nedenle düzenleyici kurumlar arasında daha güçlü koordinasyon mekanizmalarının oluşturulması önem taşımaktadır.

6.3 Yapay Zekâyı Yönetmek

Yapay zekâ teknolojilerinin hızlı gelişimi, dijital düzenleme tartışmalarını niteliksel olarak yeni bir aşamaya taşımıştır. Özellikle üretken yapay zekâ sistemlerinin yaygınlaşması, yalnızca ekonomik dönüşüm değil; hukuk, siyaset, eğitim, güvenlik ve medya alanlarında da köklü etkiler yaratmaktadır [70]. Bu nedenle yapay zekâ düzenlemeleri son yıllarda küresel dijital politika gündeminin merkezine yerleşmiş; ancak bu alana verilen yanıtlar ülkeden ülkeye köklü biçimde farklılaşmaktadır.

Avrupa Birliği tarafından geliştirilen Yapay Zekâ Yasası (AI Act), dünyanın ilk kapsamlı yapay zekâ düzenleme çerçevesi olma özelliğini taşımaktadır [34]. Düzenleme, yapay zekâ sistemlerini taşıdıkları risk düzeyine göre sınıflandırmakta; kabul edilemez risk taşıyan uygulamaları yasaklarken yüksek riskli sistemleri daha sıkı yükümlülüklerle tabi tutmaktadır. Biyometrik gözetim sistemleri, kamu hizmetlerinde kullanılan algoritmalar, sağlık sektöründeki yapay zekâ uygulamaları ve kritik altyapı sistemleri yüksek riskli kategoride değerlendirilmekte; şeffaflık, insan denetimi, veri kalitesi ve kayıt tutma yükümlülükleri bu sistemler için zorunlu kılınmaktadır [67]. AI Act'ın en tartışmalı boyutu ise Genel Amaçlı Yapay Zekâ (GPAI) sistemlerine getirilen yükümlülüklerdir. GPT-4, Gemini ve Claude gibi büyük dil modellerini geliştiren şirketler, model eğitiminde kullanılan veri setlerini açıklamak, telif hakkı uyumunu belgelemek ve belirli eşiğin üzerindeki modeller için sistematik risk değerlendirmesi yapmakla yükümlü tutulmaktadır [71]. Bu yaklaşım yapay zekâ politikalarını salt teknoloji düzenlemesinin ötesine taşıyarak bir kamusal yönetim meselesi olarak konumlandırmaktadır [72].

Amerika Birleşik Devletleri ise AB'den köklü biçimde farklı bir model benimsemektedir. ABD'nin yapay zekâ politikası, Biden döneminde çıkarılan ve kapsamlı güvenlik yükümlülükleri getiren yürütme kararnamesinin 2025 yılında yürürlükten kaldırılmasıyla yeni bir yön almıştır. Yerini alan EO 14179, düzenleme yükünü azaltarak inovasyona öncelik tanıyan bir çerçeveyi benimsemektedir. NIST Yapay Zekâ Risk Yönetim Çerçevesi ise bu süreçte temel referans belge olmayı sürdürmektedir [73, 26]. Frontier yapay zekâ şirketlerinin Beyaz Saray'a verdikleri gönüllü güvenlik taahhütleri ise bağlayıcı bir hukuki yükümlülük değil; kurumsal itibar mekanizması işlevi görmektedir. ABD'nin bu modelinin arkasında yalnızca inovasyon serbestisini koruma kaygısı değil; küresel yapay zekâ liderliğini pekiştirme stratejisi de yatmaktadır. Düzenleme yükü getirmeyen bir çerçeve, Silikon Vadisi şirketlerinin küresel rekabet üstünlüğünü koruyacak hızla geliştirme yapmasına imkân tanımaktadır [26].

Çin ise bu iki model arasında üçüncü ve kendine özgü bir konum işgal etmektedir. Çin, yapay zekâ düzenlemesine AB gibi risk sınıflandırması ya da ABD gibi öz-denetim üzerinden değil; içerik denetimi ve devlet onayı mekanizmaları üzerinden yaklaşmaktadır. 2022

tarifli Algoritmik Öneri Düzenlemesi ve 2023 tarihli Üretken Yapay Zekâ Yönetmeliđi, hizmet sunulmadan önce devlet onayını zorunlu kılmakta; üretilen içeriğın sosyalist temel değerleri yansıtmamasını şart kořmaktadır [74]. Bu model, yapay zekâyı yalnızca teknolojik bir araç olarak değıl; siyasi denetim ve toplumsal yönlendirme kapasitesinin bir parçası olarak konumlandırmaktadır.

Küresel ölçekte ise çok taraflı bir minimum standart arayışı sürmektedir. UNESCO'nun 2021 tarihli Yapay Zekâ Etiğı Tavsiye Kararı [72] ve Avrupa Konseyi'nin 2024 tarihli Yapay Zekâ Çerçeve Sözleşmesi [65] bu arayışın somut ürünleridir. Ancak bu belgeler bağlayıcı olmaktan çok yönlendirici nitelik taşımakta; uygulamayı ulusal hükümetlerin inisiyatifine bırakmaktadır. Yapay zekâ alanındaki düzenleme yarışı böylece üç farklı egemenlik anlayışının fiilen çatıştığı bir alana dönüşmektedir: AB'nin hak temelli ve zorunlu uyum modeli, ABD'nin inovasyon öncelikli öz-denetim modeli ve Çin'in devlet denetimli içerik yönetimi modeli. Hangi modelin küresel standart haline geleceğı sorusu artık yalnızca teknik bir tercih değıl; doğrudan jeopolitik bir güç meselesidir [75].

Türkiye açısından bakıldığında bu üçlü tablo hem bir risk hem de bir fırsat çerçevesi sunmaktadır. 4.3'te ayrıntılı biçimde ele alındığı üzere Türkiye'nin yapay zekâ kanun süreci henüz sonuçlanmamıştır; farklı yasa teklifleri arasındaki yaklaşım farklılıkları sürmektedir [37]. Bu belirsizliğin içinde Türkiye'nin hangi modele yakın konumlanacağı kritik bir tercih sorusu olarak öne çıkmaktadır. AB'nin AI Act yaklaşımı Türkiye'nin düzenleyici tartışmalarını doğrudan yönlendirmekte; bu durum Brüksel Etkisi'nin yapay zekâ alanında da işlediğini göstermektedir. Bununla birlikte Türkiye'nin yapay zekâ sistemlerinin kamu hizmetlerine entegrasyonu, algoritmik şeffaflık ve otomatik karar alma mekanizmalarına ilişkin kurumsal denetim kapasitesi henüz yeterli olgunluğa ulaşmamıştır. Yapay zekâ düzenlemesinde yalnızca yasal çerçeve oluşturmak değıl; bu çerçeveyi hayata geçirecek teknik uzmanlık, kurumlar arası koordinasyon ve uluslararası iş birliğı kapasitesini eş zamanlı inşa etmek Türkiye'nin önündeki temel zorluk olarak durmaktadır.

7. Türkiye İçin Politika Çerçevesi ve Stratejik Öncelikler

7.1 Dijital Egemenlik Tartışmalarında Politika İhtiyacı

Dijital egemenlik tartışmaları çoğı zaman soyut bir çerçevede ele alınmaktadır. Oysa Türkiye için mesele artık kavramsal olmaktan çıkmış; somut ve zamana karşı yarışan bir politika sorunu olarak konumlanmıştır. Kritik kamu altyapılarının yabancı sistemlerle korunduğı, bulut verilerinin yabancı hukuk çerçevelerine tabi olduğı, dijital reklam gelirlerinin büyük bölümünün yurt dışına aktığı ve telekomünikasyon omurgasının yabancı ekipmanlarla örüldüğü bir tabloda, her geçen yıl bağımlılık ilişkileri daha da derinleşmektedir. Dijital egemenliğin kaybedilmesi ani bir kırılmayla değıl; fark edilmeden biriken bağımlılıkların geri dönüşü güç bir yapıya dönüşmesiyle gerçekleşir [3]. Türkiye bu eşiğe yaklaşmaktadır.

Bu nedenle dijital egemenlik tartışmaları teknoloji karşıtı ya da içe kapanan bir perspektifle değerlendirilmemelidir. Mesele, küresel dijital ekonomiden kopmak değıl; stratejik alanlarda karar alma kapasitesini koruyabilmektir [25]. Ancak bu ayrımı yapmak, hareketsiz kalmak için bir gerekçe değıldir. Küresel sistemle bütünleşmeyi sürdürürken hangi alan-

larda daha yüksek denetim kapasitesi inşa edileceğini belirlemek; kısa, orta ve uzun vadeli öncelikleri net biçimde ortaya koymak artık bir tercih değil zorunluluktur.

Bu çerçevede Türkiye'nin dijital bağımlılık haritası üç öncelik katmanı üzerinden okunabilir. Birinci katmanda acil müdahale gerektiren alanlar yer almaktadır: kritik kamu altyapılarının siber korumasında yabancı sistem bağımlılığı ve kamu verilerinin yabancı bulut altyapılarında işlenmesi. Bu alanlardaki kırılganlıklar yalnızca ekonomik değil; doğrudan kamusal düzen ve ulusal güvenlik boyutu taşımaktadır [48]. 7545 sayılı Siber Güvenlik Kanunu ve Yerli İkame Zorunluluğu bu alanda atılmış önemli adımlardır; ancak uygulama kapasitesinin hızla güçlendirilmesi gerekmektedir. İkinci katmanda orta vadeli dönüşüm gerektiren alanlar bulunmaktadır: telekomünikasyon altyapısındaki yabancı ekipman bağımlılığının azaltılması, yerli bulut bilişim kapasitesinin stratejik sektörlerde güçlendirilmesi ve yapay zekâ alanında Türkçe veri altyapısı ile hesaplama kapasitesinin oluşturulması. Üçüncü katmanda ise yapısal dönüşüm gerektiren alanlar yer almaktadır: dijital reklam ekosisteminde yerli aktörlerin payının artırılması, platform ekonomisine özgü rekabet hukuku araçlarının geliştirilmesi ve uluslararası dijital yönetim süreçlerinde daha etkin bir konumun kazanılması [63].

Türkiye açısından temel sorunlardan biri, bu önceliklerin birbirinden kopuk biçimde ele alınmasıdır. Rekabet hukuku, veri koruma, siber güvenlik, yapay zekâ politikaları ve dijital ekonomi düzenlemeleri çoğu zaman birbirinden bağımsız alanlar gibi değerlendirilmektedir. Oysa dijital platform ekonomisinin yapısı, bu alanların giderek daha fazla iç içe geçtiğini göstermektedir [38]. Bir siber saldırı yalnızca güvenlik meselesi değil; veri egemenliği, kamu hizmeti sürekliliği ve ekonomik güvenlik meselesidir. Bir platformun veri işleme modeli yalnızca mahremiyet değil; rekabet ve ulusal güvenlik meselesidir. Bu bütüncül bakışı kurumsal yapıya yansıtabilecek koordinasyon mekanizmalarının oluşturulması, politika çerçevesinin en kritik eksiklerinden biridir [76].

Peki neden şimdi? Türkiye'nin önünde kısa ömürlü bir fırsat penceresi bulunmaktadır. 7545 sayılı Siber Güvenlik Kanunu yeni bir kurumsal kapasite zemini oluşturmuştur. Yapay Zekâ Kanun süreci henüz sonuçlanmamış; çerçeveyi şekillendirme imkânı hâlâ mevcuttur. Yerli İkame Zorunluluğu kritik sektörlerde somut bir dönüşüm başlatmıştır. Küresel ölçekte ise ABD, AB ve Çin arasındaki dijital düzenleme rekabeti standartları henüz kesinleşmemiştir; hangi modelin baskın geleceği belirsizliğini korumaktadır [75]. Bu belirsizlik Türkiye için aynı zamanda bir manevra alanıdır. Standartlar oturduğunda müdahale kapasitesi daralacaktır. Türkiye'nin bu pencereyi değerlendirip değerlendirmeyeceği, önümüzdeki birkaç yılda alınacak politika kararlarıyla belirlenecektir.

7.2 Kritik Altyapılar ve Kamu Dijital Kapasitesi

Türkiye'nin dijital egemenlik politikasının önündeki en temel engellerden biri, henüz yanıtlanmamış bir sorudur: Hangi kritik dijital altyapılar mevcuttur, bunların ne kadarı yabancı sistemlere bağımlıdır ve herhangi birinin çökmesi ya da dış müdahaleye maruz kalması halinde zincirleme olarak neler etkilenir? Bu sorunun sistematik bir yanıtı olmadan yapılacak her politika müdahalesi, gerçek kırılganlık noktalarını görmeyen kör bir müdahale olmaya mahkûmdur. Kritik dijital altyapı envanterinin çıkarılması, Türkiye'nin dijital

egemenlik yolculuğunun hem ön koşulu hem de en acil adımıdır.

Bu envanterin kapsamı geniş tutulmalıdır. Sağlık bilgi sistemleri, finansal altyapılar, enerji yönetim sistemleri, ulaşım ağları, kamu veri tabanları ve güvenlik kurumlarının dijital sistemleri bu çerçevenin temel bileşenlerini oluşturmaktadır. Bu altyapıların her birinde hangi yazılımın kullanıldığı, hangi donanımın tercih edildiği, verilerin hangi ülkede ve hangi hukuki çerçeve altında tutulduğu ve sistemin kesintiye uğraması durumunda hangi kamu hizmetlerinin etkileneceği bilinmelidir [24]. Bu bilgi olmadan öncelik sıralaması yapılamaz, kaynak tahsisi rasyonel biçimde gerçekleştirilemez ve kriz senaryolarına karşı gerçekçi bir dayanıklılık planı oluşturulamaz.

Kritik altyapıların bulut bilişim boyutu bu envanterin en hassas halkasını oluşturmaktadır. Küresel bulut pazarı Microsoft Azure, Amazon Web Services ve Google Cloud'un oligopolünde şekillenmiş durumdadır. Bu sağlayıcılara bağımlılık hem teknik hem de hukuki bir kırılabilirlik yaratmaktadır: teknik olarak kesinti riskleri küresel ölçekte yayılmakta, hukuki olarak ise CLOUD Act gibi düzenlemeler aracılığıyla yabancı hukuk sistemlerinin erişim alanını genişletmektedir [4, 44]. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin Kamu Bulut Bilişim Stratejisi taslağı kritik verilerin yurt içinde barındırılmasını temel ilke olarak benimsemiş olmakla birlikte, yurt dışı altyapılardan hizmet alımına açık bırakılan esneklik kapısı uygulamada denetim boşluğuna yol açmaktadır [44]. Bu boşluğun kapatılması; hangi verinin hangi koşulda hangi altyapıda tutulabileceğini net biçimde tanımlayan bağlayıcı bir çerçeveyi gerektirmektedir.

Bu noktada egemen bulut yaklaşımları önemli bir politika aracı olarak öne çıkmaktadır. Fransa'nın Bleu girişimi, Microsoft ve Google'ın Fransız ortaklarıyla kurduğu yapı aracılığıyla kamu verilerinin Fransız hukuku altında ve Fransız denetiminde tutulmasını sağlamaktadır. Avrupa'nın Gaia-X projesi ise birden fazla ülkenin katılımıyla ortak bir veri altyapısı ve güven çerçevesi oluşturmayı hedeflemektedir [77]. Bu modeller Türkiye için doğrudan kopyalanabilir şablonlar değildir; ancak kamu verisi ile ticari bulut hizmetleri arasındaki dengeyi nasıl kurabileceğine dair değerli bir çerçeve sunmaktadır. Türkiye'nin bu alanda tercih edeceği model, yalnızca teknik bir karar değil; egemenlik anlayışını somutlaştıran bir politika tercihi olacaktır.

Açık kaynak yazılım ekosistemleri bu politika çerçevesinin kritik ama yeterince değerlendirilmeyen bir boyutunu oluşturmaktadır. Açık kaynak çözümler yalnızca maliyet avantajı sağlamaz; daha önemlisi, yazılımın kaynak kodunun denetlenebilmesine, bağımsız güvenlik değerlendirmesi yapılabilmesine ve mülkiyet bağımlılığından çıkılabilmesine imkân tanır. Kapalı kaynak bir güvenlik yazılımında hangi arka kapıların bulunduğunu doğrulamak teknik olarak mümkün değildir. Bu nedenle kritik kamu altyapılarında açık kaynak tercihini teşvik eden ya da belirli alanlarda zorunlu kılan bir politika çerçevesi, dijital egemenliğin somut bir güvencesi haline gelebilir [63].

Kamu dijital kapasitesinin güçlendirilmesinde uluslararası deneyimler yol gösterici olmaktadır. Estonya'nın X-Road veri alışveriş katmanı, farklı kamu kurumlarının verilerini güvenli biçimde birbirleriyle paylaşmasını sağlayan açık kaynaklı bir altyapı olarak dikkat çekmektedir. Dijital kimlik sistemi ve e-Residency uygulamasıyla bütünleşen bu yapı, kamu

hizmetlerinin bütünleşik ve kesintisiz biçimde sunulmasının teknik zeminini oluşturmaktadır. Hindistan'ın Aadhaar sistemi ise 1,4 milyarlık bir nüfusa ölçeklenen dijital kimlik doğrulama, ödeme altyapısı ve kamu hizmeti entegrasyonunun bir arada çalıştığı en kapsamlı Dijital Kamu Altyapısı (Digital Public Infrastructure, DKA) örneği olarak öne çıkmaktadır. Bu modellerin ortak özelliği, kamu hizmetlerinin özel platformların inisiyatifine bırakılmak yerine açık standartlar ve kamusal denetim altında inşa edilmesidir [78].

Türkiye açısından kamu dijital kapasitesinin güçlendirilmesi yalnızca teknik altyapı yatırımlarıyla sınırlı değildir. Kamu kurumlarında dijital sistemleri anlayan, değerlendiren ve denetleyebilen teknik uzmanlık kapasitesinin oluşturulması en az altyapının kendisi kadar kritiktir. Yabancı bir sistemin güvenlik açığını tespit edecek kapasitesi olmayan bir kurum, o sistemin raporladığı güvenlik durumuna körü körüne güvenmek zorunda kalmaktadır. Bu yapısal bağımlılığı kırmak, önce insan kaynağına yatırımı, ardından kurumlar arası teknik koordinasyon mekanizmalarının oluşturulmasını gerektirmektedir [76].

Türkiye Yapay Zekâ Eylem Planı (2026-2030), kritik altyapı ve kamu dijital kapasitesi tartışmasına “Rekabetçi ve düşük karbonlu bir ulusal hesaplama omurgası kurulması” başlıklı beşinci eylemi aracılığıyla altyapı ve yatırım boyutuyla doğrudan katkı sağlamaktadır. Plan; 2030 yılına kadar Türkiye'nin en az 1 GW yapay zekâ/veri merkezi kurulu gücüne, yıllık en az 10 TWh düşük karbonlu elektrik satın alma anlaşması (PPA) hacmine, en az 1 eksabayt depolama kapasitesine ve omurga bağlantılarında en az 100 Tb/sn erişime ulaşılmasını hedeflemektedir. Bu kapasitenin finansmanı için en az 10 milyar ABD doları tutarında, özel sektör ağırlıklı bir yatırımın mobilize edilmesi öngörülmekte; bu mobilizasyon HIT-30 Yüksek Teknoloji Yatırım Programı kapsamında ilan edilecek Veri Merkezi ve Yapay Zekâ çağrılılarıyla teşvik edilecektir. Araştırmacılar, girişimler ve KOBİ'ler için dünya standartlarında hesaplama kapasitesinin doğrudan erişime açılması ve tek bir sağlayıcıya bağımlılığı önlemek amacıyla çoklu tedarikçi yaklaşımının benimsenmesi, bu bölümde vurgulanan yerli ve denetlenebilir altyapı ihtiyacıyla örtüşen bir yaklaşımdır.

Bu hedefler, bu bölümde vurgulanan yerli ve egemen hesaplama kapasitesi ihtiyacına doğrudan yanıt üretme potansiyeli taşımaktadır. Planın dikkat çekici yönlerinden biri, veri merkezi kapasitesinin yalnızca kurulu güç olarak değil; enerji verimliliği ve sürdürülebilirlik göstergeleriyle birlikte ele alınmasıdır. Nitekim metinde, sözleşmelerde en az %60 düşük karbonlu (yenilenebilir veya nükleer) elektrik şartı, Güç Kullanım Etkinliği (PUE) ve Su Kullanım Etkinliği (WUE) performansı, şebeke bağlantı kapasitesi ve atık ısının geri kazanımı gibi ölçütler tanımlanmakta; yapay zekâ altyapısının artan enerji talebinin ulusal enerji sistemiyle uyumlu biçimde planlanması Ulusal Yapay Zekâ Kurulu'nun öncelikli gündem maddelerinden biri olarak konumlandırılmaktadır. Bu yaklaşım, altyapı hedeflerinin enerji politikalarıyla eşgüdüm içinde yürütülmesi gerektiği yönündeki tespitle uyumludur. Kapasitenin yalnızca kurulması değil; araştırma ve girişim ekosisteminin erişimine token bazlı ve şeffaf biçimde tahsis edilmesi ise, bu bölümde vurgulanan kamusal denetim ve teknik uzmanlık kapasitesiyle birlikte ele alınması gereken bir yönetim meselesi olmayı sürdürmektedir.

7.3 Rekabet Hukuku ve Dijital Piyasalar

Türkiye'nin dijital piyasalara yönelik rekabet hukuku çerçevesi köklü bir güncelleme ihtiyacı içindedir. 4054 sayılı Rekabetin Korunması Hakkında Kanun, fiyat artışları ve tüketici zararı ekseninde, ihlal gerçekleşikten sonra devreye giren bir müdahale mantığıyla tasarlanmıştır. Dijital piyasalarda ise bu mantık işlememektedir. Ağ etkileri ve veri yoğunlaşması, piyasayı rekabet kurumları müdahale etmeden çok önce kilitlemektedir. Bir platform kritik kullanıcı kitlesine ve veri birikimine ulaştıktan sonra rakiplerin pazara girişi fiilen imkânsız hale gelebilmektedir [9]. Başka bir deyişle geleneksel rekabet hukuku araçları dijital piyasalarda her zaman zarar oluştuktan sonra devreye girmekte; ancak bu noktada yapısal dönüşümü geri almak çoğu zaman mümkün olamamaktadır [53].

Bu gecikmenin somut maliyeti vardır. Uygulama mağazaları üzerinden alınan yüksek komisyonlar yerli yazılım şirketlerinin ölçeklenmesini kısıtlamaktadır. Arama motoru algoritmaları rakip hizmetleri görünmez kılarken kendi hizmetlerini öne çıkarmaktadır. Dijital reklam teknolojileri piyasası birkaç küresel aktörün kontrolünde şekillenirken yerli medya organları bu yapıya bağımlı hale gelmektedir. Rekabet Kurumu son yıllarda Google hakkında arama motorları, reklam teknolojileri ve Android ekosistemi alanlarında önemli soruşturmalar başlatmıştır [55]. Bu adımlar değerlidir; ancak soruşturmaların uzun sürmesi ve yapısal çözümler yerine para cezalarıyla sonuçlanma riski, ihlal sonrası müdahale modelinin sınırlarını gözler önüne sermektedir.

Avrupa Birliği bu soruna *ex ante* yani ihlal gerçekleşmeden önce devreye giren düzenleme yaklaşımıyla yanıt vermiştir. Dijital Piyasalar Yasası belirli ölçeğin üzerindeki platformları “kapı bekçisi” olarak tanımlamakta ve bu şirketlere özel yükümlülükler getirmektedir: kendi hizmetlerini öne çıkarmama, alternatif uygulama mağazalarına izin verme, veri taşınabilirliği sağlama ve birlikte çalışabilirlik standartlarına uyma [11]. Türkiye AB üyesi olmadığından DMA doğrudan uygulanamamaktadır. Ancak burada kritik bir asimetri söz konusudur: Türkiye’de faaliyet gösteren kapı bekçisi platformlar AB pazarında DMA yükümlülüklerine tabi iken Türkiye pazarında bu yükümlülüklerin karşılığı bulunmamaktadır. Aynı platform Türk kullanıcılara karşı Avrupalı kullanıcılara kıyasla çok daha az kısıtlamayla faaliyet göstermektedir. Bu yapısal eşitsizlik Türkiye’nin dijital piyasa düzenlemesindeki gecikmenin doğrudan bir maliyetidir.

Dijital piyasalardaki egemenlik açığı yalnızca rekabet hukuku boyutuyla sınırlı kalmamaktadır. Vergi egemenliği de bu tablonun kritik bir bileşenini oluşturmaktadır. Türkiye, 2020 yılında yürürlüğe giren düzenlemeyle yabancı dijital platformların Türkiye’deki kullanıcılardan elde ettikleri gelirler üzerinden yüzde 7,5 oranında Dijital Hizmet Vergisi uygulamaya koymuştur [79]. Bu adım, dijital ekonominin vergisel boyutunda egemenlik talebinin somut bir ifadesidir. Bununla birlikte düzenlemenin uygulamadaki etkinliği yapısal kısıtlarla karşı karşıyadır. Google, Meta ve Netflix gibi küresel platformlar Türkiye’de fiziksel bir yerleşik varlık oluşturmaksızın faaliyet göstermekte; Türkiye’deki reklam ve içerik gelirlerini çoğunlukla düşük vergi rejimlerine sahip Avrupa ülkelerindeki holding yapıları üzerinden muhasebelemektedir. Transfer fiyatlandırması mekanizmaları aracılığıyla Türkiye’de üretilen dijital değer önemli bir bölümü vergilendirilebilir gelir olarak Türkiye’de kalmamaktadır. OECD’nin dijital ekonomide vergi tabanı erozyonuna ilişkin kapsamlı

çalışmaları bu sorunun yalnızca Türkiye'ye özgü olmadığını; küresel ölçekte yapısal bir dönüşüm gerektirdiğini ortaya koymaktadır [80]. Türk vergi otoritelerinin bu yapıyı bağımsız biçimde denetleyebilme kapasitesi ise oldukça sınırlıdır. Sonuç olarak Dijital Hizmet Vergisi doğru bir politika aracı olmakla birlikte, denetim kapasitesi ve uluslararası vergi iş birliği mekanizmaları olmadan tam anlamıyla işlevini yerine getirememektedir.

Bu tablo, dijital hegemonyayı doğrudan besleyen bir döngüyü gözler önüne sermektedir. Küresel platformlar Türkiye pazarından değer üretmekte; bu değer hem rekabetçi hem de vergisel karşılığını tam olarak ödemediği faaliyetlerini sürdürmektedir. Böylece yerli aktörler eşitsiz rekabet koşullarında faaliyet gösterirken devlet de kendi topraklarında yaratılan dijital değer üzerinde tam egemenlik uygulayamamaktadır. Bu durum yalnızca ekonomik bir kayıp değil; dijital platformların piyasa gücünü ve vergi optimizasyon kapasitesini devletin düzenleme ve vergilendirme yetkisinin önüne geçirdiği yapısal bir egemenlik erozyonudur [3].

Türkiye açısından değerlendirilmesi gereken politika araçları bu çerçevede netleşmektedir. Birincisi, kapı bekçisi niteliğindeki platformlara yönelik sektöre özgü ex ante yükümlülüklerin 4054 sayılı Kanun çerçevesinde ya da ayrı bir dijital piyasalar mevzuatıyla hayata geçirilmesidir [16]. İkincisi, veri paylaşım yükümlülüklerinin gündeme alınmasıdır. AB'nin Veri Yasası ve Veri Yönetişimi Yasası platform verilerinin belirli koşullar altında üçüncü taraflarla paylaşılmasını zorunlu kılmaktadır [81, 82]. Türkiye'de bu mekanizma henüz mevcut değildir. Üçüncüsü, Dijital Hizmet Vergisi'nin etkinliğini artıracak denetim altyapısının güçlendirilmesi ve OECD'nin küresel asgari kurumlar vergisi çerçevesiyle uyumun derinleştirilmesidir [79, 80]. Dördüncüsü ise Rekabet Kurumu'nun dijital kapasite yatırımlarına öncelik vermesidir. Algoritmik sistemleri, veri ekonomisini ve platform ekosistemlerini anlayan teknik uzman kadrosunun oluşturulması, dijital piyasaların etkin biçimde denetlenebilmesinin kurumsal ön koşuludur [55].

Rekabet hukuku ve vergi egemenliği reformu Türkiye'nin dijital egemenlik politikasının ayrı bileşenleri olarak değil; bütünün birbirini tamamlayan parçaları olarak ele alınmalıdır. Piyasa yapısını şekillendiremediği gibi kendi topraklarında üretilen dijital değeri tam olarak vergilendirecek kapasiteden yoksun bir devlet, platformların belirlediği koşullarla yaşamak zorunda kalır. Yerli aktörlerin büyüyelebileceği, yenilik yapabileceği ve ölçeklenebileceği rekabetçi bir dijital piyasa ortamı oluşturmak; hem ekonomik hem de egemenlik boyutuyla stratejik bir önceliklerdir [54].

Bu bölümde ele alınan politika araçlarının bir bölümü, Türkiye Yapay Zekâ Eylem Planı'nın yaklaşımıyla aynı yönde ilerlemektedir. Planın düzenleyici çerçeveyi yeniliği yavaşlatmayan, güvenli ölçeklemeyi mümkün kılan bir güven altyapısı olarak konumlandırması; Algoritmik Etki Değerlendirmesi, Model Kartı ve sektörel düzenleyici deney alanları (regulatory sandbox) gibi araçları öngörmesi ve düzenleyici kurumların teknik kapasitesinin güçlendirilmesini hedeflemesi, bu çalışmada savunulan kurumsal kapasite önceliğiyle örtüşmektedir. Öte yandan planın ağırlık merkezi; üretim, altyapı, yetenek ve yerli model geliştirme eksenlerinde yoğunlaşmakta, düzenlemeyi ise büyük ölçüde bu ekosistemi mümkün kılan bir güven çerçevesi olarak ele almaktadır. Bu çalışmanın öne çıkardığı kapı bekçisi

platformlara yönelik ex ante yükümlülükler, platform verilerinin paylaşımına ilişkin bağlayıcı mekanizmalar ve dijital hizmet vergisinin denetim kapasitesinin güçlendirilmesi gibi öncelikler ise, planın kapsadığı alanı platform gücünün dengelenmesi ve vergi egemenliği boyutlarıyla tamamlayan bir gündem oluşturmaktadır. Bu iki yaklaşımın bütünleştirilmesi; yani üretim ve altyapı odaklı kapasite inşasının, platformlara yönelik düzenleyici araçlarla eşzamanlı yürütülmesi, Türkiye'nin dijital egemenlik hedefi açısından bütüncül bir çerçeve sunacaktır.

7.4 Veri Yönetişimi ve Yapay Zekâ Politikaları

Yapay zekâ kapasitesi temelde bir veri meselesidir. Hangi ülkenin daha büyük, daha çeşitli ve daha kaliteli veri birikimini işleyebildiği; hangi ülkenin bu veriyi anlamlı modellere dönüştürebildiği, yapay zekâ alanındaki güç dağılımını doğrudan belirlemektedir [33]. Bu çerçevede Türkiye'nin en az değerlendirilen stratejik varlığı, devletin onlarca yıl boyunca biriktirdiği kamu verisidir. Sağlık kayıtları, nüfus verileri, ulaşım örüntüleri, eğitim çıktıları ve vergi bilgileri; doğru bir yönetim çerçevesiyle işlendiğinde Türkiye'nin yerli yapay zekâ ekosistemini besleyebilecek eşsiz bir hammadde oluşturmaktadır. Bu kapasitenin kullanılmaması yalnızca bir fırsat kaybı değil; aynı zamanda yerli aktörlerin yabancı veri tekellerine olan bağımlılığını pekiştiren yapısal bir tercih anlamına gelmektedir.

Kamu verisinin araştırmacılara ve yerli şirketlere belirli koşullar altında erişilebilir kılınması bu bağlamda birincil politika önceliği olmalıdır. AB'nin Veri Yönetişimi Yasası, kamu kurumlarının elindeki verilerin yeniden kullanımını kolaylaştıran güven mekanizmalarını ve aracı kurumları düzenlemekte; veri erişimini hak temelli bir çerçeveye oturtmaktadır [82]. Türkiye'de benzer bir mekanizma henüz mevcut değildir. Kamu kurumları arasında bile veri paylaşımı çoğu zaman kurumsal engeller ve teknik uyumsuzluklar nedeniyle gerçekleşmemektedir. Ortak veri standartları, birlikte çalışabilirlik protokolleri ve güvenli veri paylaşım platformlarının oluşturulması bu sorunun teknik çözümüdür. Ancak asıl mesele teknik değil yönetimseldir: hangi verinin kimlerle, hangi koşullar altında ve hangi denetim mekanizmaları çerçevesinde paylaşılacağına ilişkin net bir politika çerçevesi bulunmamaktadır [78].

Bu değerlendirmede öne çıkan yönetim ihtiyacının önemli bir bölümü, Türkiye Yapay Zekâ Eylem Planı'nda karşılık bulmaktadır. Planın "Veri temelli yapay zekâ atılımı" başlıklı üçüncü eylemi; Ulusal Veri Kütüphanesi, Veri Alanları ve Güvenli Veri Paylaşım Programı ile bir Açık Veri Politikası aracılığıyla kamu veri setlerinin makine okunabilir, standart meta veri ve lisans bilgisiyle erişime açılmasını; ayrıca ortak veri standartlarının, birlikte çalışabilirlik protokollerinin ve bir Veri Fabrikası işlevinin oluşturulmasını öngörmektedir. Bu yönüyle plan, yukarıda tarif edilen teknik çözümün büyük ölçüde politika gündemine alındığını göstermektedir. Bununla birlikte bu çalışmada vurgulanan asıl mesele, yani veri paylaşımının hak temelli bir çerçeveye oturtulması ve bağımsız bir denetim mimarisiyle desteklenmesi, planın uygulama aşamasında somutlaşması gereken bir boyut olmayı sürdürmektedir. Dolayısıyla plan bu alanda güçlü bir başlangıç çerçevesi sunmakta; bu çalışmanın önerileri ise söz konusu çerçevenin denetlenebilirlik ve öngörülebilirlik boyutlarını tamamlayıcı nitelik taşımaktadır.

Türkçe büyük dil modeli meselesi bu tartışmanın en somut ve en acil boyutunu oluşturmaktadır. Ulusal Yapay Zekâ Stratejisi'nin öncelikleri arasında yer alan yerli Türkçe büyük dil modeli geliştirme hedefi [35], yalnızca teknolojik bir tercih değil; doğrudan bir dijital ege-menlik meselesidir. Türkçe için özelleştirilmiş ve yeterli ölçekte eğitilmiş bir model mevcut olmadığında, Türkçe konuşan kullanıcıların dil anlayışı, kültürel bağlamı ve toplumsal değerleri yabancı modellerin tasarım tercihlerine ve eğitim verilerine tabi hale gelmektedir. Bir dil modeli yalnızca kelime üretmez; anlam çerçeveleri, öncelik hiyerarşileri ve kültürel varsayımlar taşır. Bu modellerin kimler tarafından, hangi verilerle ve hangi değer yargıları-yla eğitildiği, kullanıcıların aldığı yanıtları ve dolayısıyla bilişsel çerçevelerini doğrudan şekillendirmektedir [8]. Bu doğrultuda, TÜBİTAK BİLGEM tarafından geliştirilen BİLGE Büyük Dil Modeli, Türkiye'nin yerli yapay zekâ kapasitesi açısından önemli bir başlangıç niteliği taşımaktadır. 2026 Türkiye Yapay Zekâ Eylem Planı kapsamında kamu hizmetlerinde öncelikli olarak değerlendirilmesi ve zaman içinde farklı kullanım alanlarına yaygınlaştırılması öngörülen BİLGE, Türkçenin dil yapısını, kültürel bağlamını ve kamu ihtiyaçlarını gözetten bir temel model geliştirme yaklaşımını temsil etmektedir. Bu nedenle, BİLGE'nin başarısı yalnızca teknik performansıyla değil; kamu verisine erişim, araştırma altyapısı, açık kaynak katkıları ve özel sektör tarafından benimsenme düzeyiyle de ölçülmelidir. Bununla birlikte, gerçek etki yalnızca tek bir model geliştirilmesiyle değil; bu model etrafında açık veri ekosisteminin, araştırmacı topluluğunun, uygulama geliştiricilerinin ve özel sektörün katılımını sağlayacak sürdürülebilir bir inovasyon ekosisteminin oluşturulmasıyla mümkün olacaktır.

Yapay zekâ sistemlerinin kamu hizmetlerine entegrasyonu ise algoritmik hesap verebilirlik meselesini gündeme taşımaktadır. Sosyal yardım başvurularını değerlendiren, vergi incelemesi önceliklendiren ya da güvenlik risk değerlendirmesi yapan yapay zekâ sistemleri; şeffaflık, itiraz hakkı ve insan denetimi mekanizmaları olmaksızın işletildiğinde ciddi hak ihlali riskleri barındırmaktadır [72]. Türkiye'de kamu kurumlarında kullanılan algoritmik sistemlere ilişkin kapsamlı bir envanter, denetim çerçevesi ya da vatandaş başvuru mekanizması henüz mevcut değildir. Bu boşluk, yapay zekâ kanun sürecinin [37] en öncelikli gündem maddelerinden birini oluşturmaktadır. AB'nin AI Act'inde yüksek riskli kategori olarak tanımlanan kamu hizmetleri alanındaki algoritmik uygulamalar için öngörülen şeffaflık ve insan denetimi yükümlülükleri, Türkiye'nin bu alandaki çerçevesini geliştirirken değerli bir referans oluşturmaktadır [34].

Türkiye'nin yapay zekâ alanında anlamlı bir kapasite inşa edebilmesi için uluslararası iş birliği de stratejik bir araç olarak değerlendirilmelidir. En ileri düzey (frontier) yapay zekâ modellerini geliştirmek için gereken hesaplama gücü ve veri birikimi kısa vadede tek başına elde edilebilecek düzeyin ötesindedir. Ancak bu, Türkiye'nin küresel yapay zekâ ekosisteminde yalnızca tüketici konumuna mahkûm olması gerektiği anlamına gelmemektedir. Ortak Türkçe veri havuzlarının oluşturulması, açık kaynak model geliştirme süreçlerine katkı sağlanması ve bölgesel araştırma ortaklıklarının kurulması; Türkiye'nin sınırlı kaynakları en etkin biçimde değerlendireceği alanlardır [63]. Bu yaklaşım aynı zamanda Türkiye'yi uluslararası yapay zekâ yönetim süreçlerinde daha güçlü bir konuma taşıyacak; standart belirleme tartışmalarında söz sahibi olma kapasitesini artıracaktır [65].

Veri yönetiřimi ve yapay zekâ politikaları birbirinden bağımsız teknik alanlar olarak değil; Türkiye'nin dijital egemenlik stratejisinin birbirine kenetlenmiş iki bileřeni olarak ele alınmalıdır. Veri olmadan yapay zekâ kapasitesi kurulamaz; yapay zekâ politikası olmadan veri stratejik bir varlığa dönüřtürülemez. Bu bütünleşik yaklaşımı kurumsal yapıya yansı-tacak koordinasyon mekanizması ise hem Cumhurbaşkanlığı Dijital Dönüřüm Ofisi hem de ilgili bakanlıklar arasında henüz tam anlamıyla oluşturulamamıştır [76].

Türkiye Yapay Zekâ Eylem Planı (2026-2030), bu bölümde ortaya konulan veri yönetiři-mi ve yapay zekâ politikası önceliklerinin önemli bir bölümünü resmî politika gündemine taşımıştır. Planın en az iki bin kamu veri setinin Ulusal Veri Kütüphanesi aracılığıyla arařtır-macıların, girişimlerin ve kamu kurumlarının erişimine açılmasını öngörmesi; bu çalış-ma-da kamu verisinin en az deęerlendirilen stratejik varlık olarak nitelendirilen yaklaşımıyla doğrudan örtüşmektedir. Benzer biçimde, kamu yatırım programlarında yapay zekâ proje-lerine belirli bir asgari pay ayrılması ve kamu kurumlarının yerli çözümler için ilk kullanıcı ve referans müşteri rolü üstlenmesi yönündeki hedefler; yerli ekosistemin ölçeklenmesinde kamunun kaldıraç işlevini güçlendirebilecek somut araçlardır.

Bununla birlikte, kamu veri setlerinin erişime açılması ile bu verilerin nitelikli, birlik-te çalışabilir ve kullanıma hazır hâle getirilmesi arasındaki farkın, uygulamanın başarısını belirleyecek kritik bir eşik olduęu göz ardı edilmemelidir. Ortak veri standartları, birlikte çalışabilirlik protokolleri ve güvenli paylaşım altyapılarıyla desteklenmedięi takdirde, veri setlerinin sayısal olarak açılması tek başına yeterli bir sonuç üretmeyebilir. Yerli büyük dil modeli boyutunda ise plan, bu bölümde deęerlendirilen yaklaşımı pekiřtirmekte; Türkçe büyük dil modeli çalışmalarının dijital egemenlik hedefiyle sürdürülmesini ve kamu hiz-metlerinde önceliklendirilmesini öngörmektedir. Bu doğrultuda TÜBİTAK, T3 Vakfı-Baykar iş birlięi ve HAVELSAN gibi kurum ve girişimler tarafından yürütölen yerli model çalış-maları, tek bir modelin ötesinde sürdürülebilir bir inovasyon ekosistemi hedefiyle birlikte de-ęerlendirilmektedir.

7.5 Dijital Egemenlik ve Uluslararası İş Birlięi

Dijital egemenlik tartışmaları çoęu zaman ulusal kapasite inřası ekseninde ele alınmak-tadır. Oysa küresel dijital ekonominin yapısı, hiçbir ülkenin bu alanda yalnız başına yeterli bir konum elde edemeyeceęini göstermektedir. Standartlar, protokoller, veri aktarım kural-ları ve yapay zekâ yönetiřim çerçeveleri uluslararası süreçlerde şekillenmektedir. Bu süreç-lere katılmayan ya da yalnızca izleyici konumunda kalan ölkeler, başkalarının belirledięi kurallarla yaşamak zorunda kalmaktadır [83]. Türkiye bugün tam olarak bu konumdadır: GDPR'ye uyum sağlamakta, AI Act'in etkilerini takip etmekte, DMA'nın dolaylı yansımalarını yönetmektedir. Ancak bu standartların hiçbirinin belirlenmesinde anlamlı bir rol üstlenme-miştir. Reaktif konumdan proaktif konuma geçiř, Türkiye'nin uluslararası dijital yönetiřim-deki en temel dönüřüm ihtiyacıdır.

Bu dönüřümün önündeki ilk engel kurumsal kapasitedir. Dijital yönetiřim müzakerele-rine etkin biçimde katılabilmek için teknik uzmanlık, diplomatik kapasite ve kurumlar arası koordinasyon gerekmektedir. OECD Dijital Ekonomi Politika Komitesi, BM İnternet Yöneti-řim Forumu, ITU ve G20 Dijital Ekonomi Çalışma Grubu gibi platformlarda Türkiye'nin var-

lığı sınırlı kalmaktadır. Bu platformlarda yapay zekâ standartları, veri akışı kuralları, siber güvenlik normları ve dijital vergilendirme gibi konularda alınan kararlar, Türkiye’yi doğrudan etkileyen sonuçlar doğurmaktadır [63]. Etkilenen taraf olarak müzakere masasında yer almak ile bu masada şekillendirici bir aktör olarak bulunmak arasındaki fark, ülkenin uzun vadeli dijital egemenlik kapasitesini belirleyecektir.

Türkiye açısından AB ile ilişki bu tablonun en kritik boyutunu oluşturmaktadır. Türkiye AB üyesi olmadığından AB’nin dijital düzenlemeleri doğrudan uygulanamamaktadır. Ancak gerçekte durum çok daha karmaşıktır: Türkiye’de faaliyet gösteren küresel platformlar AB pazarında GDPR, DMA ve AI Act yükümlülüklerine tabidir. Bu yükümlülükler fiilen bu platformların küresel operasyonel modellerini şekillendirmekte; Türkiye de bu modelin dolaylı alıcısı konumuna düşmektedir. Avrupa Birliği standartlarına uyum yalnızca hukuki bir mesele değil; Türkiye’nin en büyük ticaret ortağıyla ekonomik entegrasyonunun sürdürülebilirliği meselesidir [84]. Bu nedenle AB’nin dijital düzenleme gündemini takip eden, etki analizleri yapan ve müzakere kapasitesini geliştiren kurumsal bir yapının oluşturulması stratejik bir zorunluluktur.

Türkiye’nin özellikle değerlendirmesi gereken bir fırsat alanı bölgesel liderlik kapasitesidir. Coğrafi konumu, ekonomik büyüklüğü ve köprü ülke niteliğiyle Türkiye, Orta Asya, Orta Doğu ve Balkanlar’ı kapsayan geniş bir coğrafyada dijital yönetim alanında referans ülke olma potansiyeline sahiptir. Bu bölgelerdeki ülkeler dijital altyapı, siber güvenlik ve veri yönetimi alanlarında model arayan; ancak ne AB’nin kurumsal çerçevesine tam uyum sağlayabilen ne de ABD veya Çin modellerini bütünüyle benimseyebilen ülkelerdir. Türkiye’nin bu boşlukta geliştireceği ikili ve çok taraflı dijital iş birliği mekanizmaları hem bölgesel etkisini güçlendirecek hem de uluslararası dijital yönetim süreçlerindeki görünürlüğünü artıracaktır [25].

Türkiye Yapay Zekâ Eylem Planı (2026-2030), bu bölümde vurgulanan proaktif uluslararası konumlanma ihtiyacına yönelik somut yönelimler içermektedir. Plan; OECD, G20 ve Birleşmiş Milletler gibi platformlarda insan merkezli yapay zekâ standartlarının oluşumuna katkı verilmesini, İstanbul’un yapay zekâ yatırımları ve girişimcilik açısından uluslararası bir vitrin hâline getirilmesini ve uluslararası girişimcilere tek pencereden hızlandırılmış bir yol haritası sunulmasını öngörmektedir. Bu yönelimler, raporda tanımlanan “reaktif konumdan proaktif konuma geçiş” ihtiyacıyla uyumludur.

Planın bölgesel liderlik boyutundaki en dikkat çekici unsuru ise, Türk Devletleri Teşkilatı, D-8 ve İslam İşbirliği Teşkilatı gibi çok taraflı platformlar çerçevesinde Türk dillerini kapsayan ortak bir büyük dil modeli ile bölgesel bir yatırım bankası geliştirilmesi hedefidir. Söz konusu modelin Oğuz, Kıpçak ve Karluk dil ailelerini kapsayacak ve üye devletlerin yüksek başarılı hesaplama altyapılarıyla birlikte geliştirilecek biçimde tasarlanması öngörülmektedir. Bu hedef, teknik bir model geliştirme girişiminin ötesinde; ortak bir dil ve veri alanının oluşturulması yoluyla bölgesel iş birliğini derinleştirme ve Türkiye’nin bu coğrafyada dijital yönetim alanında referans kapasitesini güçlendirme potansiyeli taşımaktadır. Öte yandan plan, çok taraflı iş birliğini yalnızca bölgesel ölçekle sınırlamamakta; Türkiye’nin Dijital Avrupa Programı ve EuroHPC Ortak Girişimi’ne katılımcı ülke olarak yer alması ile

OECD, G20 ve Birleşmiş Milletler platformlarında insan merkezli standartların oluşumuna katkı vermesini bir arada öngörmektedir. Uluslararası yeteneğin çekilmesine yönelik olarak tek dijital başvuru ekranı üzerinden işleyen hızlandırılmış bir yetenek vizesi (TechVisa) mekanizmasının tanımlanması da bu proaktif konumlanmanın somut araçlarından biridir. Bu çalışmada vurgulanan köprü ülke niteliği ve bölgesel referans olma fırsatı, söz konusu hedeflerle somut bir ifade kazanmaktadır.

Siber güvenlik alanındaki uluslararası iş birliği bu çerçevenin özellikle acil bir bileşenini oluşturmaktadır. Siber tehditler ulusal sınırları tanımamakta; saldırı vektörleri, kötü amaçlı yazılım altyapıları ve devlet destekli siber operasyonlar birden fazla ülkeyi eş zamanlı olarak etkilemektedir. 7545 sayılı Siber Güvenlik Kanunu'nun kurumsal zeminini oluşturduğu Siber Güvenlik Başkanlığı'nın NATO, AB Siber Güvenlik Ajansı (ENISA) ve ilgili ülkelerle ikili iş birliği protokollerini güçlendirmesi, Türkiye'nin siber dayanıklılık kapasitesinin uluslararası boyutunu pekiştirecektir [24, 48].

Dijital egemenlik nihai tahlilde yalnızca sınırlar içinde inşa edilemez. Hangi verilerin serbest dolaşabileceği, hangi yapay zekâ sistemlerinin güvenilir sayılacağı, hangi platformların hangi yükümlülöklere tabi olacağı ve hangi siber normların evrensel geçerlilik kazanacağı — bu soruların yanıtları uluslararası arenada şekillenmektedir. Türkiye bu arenada daha güçlü, daha hazırlıklı ve daha proaktif bir konumla yer aldığında, dijital egemenliği yalnızca savunulacak değil; aynı zamanda şekillendirilecek bir kapasite haline gelecektir [3].

8. Sonuç

Dijital teknolojiler son yirmi yıl içinde yalnızca ekonomik üretim biçimlerini değil; devletlerin yönetim kapasitesini, toplumların bilişsel çerçevelerini ve uluslararası güç dengelerini köklü biçimde dönüştürmüştür [1]. Bu dönüşümün özünde, dijital platformların artık yalnızca ticari aktörler olmaktan çıkıp modern toplumların vazgeçilmez altyapı bileşenlerine dönüşmesi yatmaktadır [38]. Arama motorları, sosyal medya platformları, bulut bilişim altyapıları ve yapay zekâ sistemleri; ekonomik faaliyetlerin, kamusal iletişimin ve devlet kapasitesinin işlediği zemindir. Bu zemini kim inşa ediyorsa, kim işletiyorsa ve kim denetliyorsa; hegemonyanın gerçek sahibi de giderek o olmaktadır.

Bu çalışmanın temel argümanı, dijital hegemonyanın tek boyutlu bir güç olgusu olmadığıdır. Hegemonya artık üç katmanlı ve birbirini besleyen bir yapıya sahiptir. Birinci katmanda piyasa gücü yer almaktadır: ağ etkileri, veri yoğunlaşması ve ekosistem bağımlılığı aracılığıyla sınırlı sayıdaki platform küresel ölçekte rakipsiz bir konum edinmektedir [7]. İkinci katmanda devlet-teknoloji füzyonu bulunmaktadır: Palantir'in ABD istihbarat kurumlarına entegrasyonu, Microsoft'un Pentagon bulut altyapısı ve Anduril liderliğindeki savunma teknolojisi konsorsiyumunun yükselişi; özel şirketlerin devlet kapasitesinin ayrılmaz bir parçasına dönüştüğünü göstermektedir [18, 22]. Üçüncü katmanda ise hukuki yetki alanının sınır ötesine taşınması bulunmaktadır. CLOUD Act gibi düzenlemeler aracılığıyla ulusal hukuk, küresel teknoloji şirketlerinin faaliyet gösterdiği her coğrafyaya uzanabilmektedir [4]. Böylece dijital platformların ekonomik üstünlüğü, devletlerin stratejik kapasitesi ve hukuk düzenlerinin coğrafi etkisi tek bir mimari içinde birleşmektedir.

Bu çerçevede dijital hegemonya, klasik emperyalizm veya ekonomik bağımlılık tartışmalarından farklılaşmaktadır. Geçmişte jeopolitik üstünlük; enerji kaynaklarının, deniz yollarının veya askeri üslerin kontrolü üzerinden açıklanırken, günümüzde veri merkezleri, bulut altyapıları, yarı iletken tedarik zincirleri, algoritmalar ve yapay zekâ modelleri yeni güç projeksiyonunun araçları haline gelmiştir. Egemenlik artık yalnızca toprağı kontrol etmekle değil; bilgi akışını, hesaplama kapasitesini ve dijital altyapıyı yönetebilmekle de ölçülmektedir. Dolayısıyla dijital dönüşüm yalnızca teknolojik bir gelişme olarak ele alınamayacaktır, bilakis dijital hegemonya uluslararası sistemin güç mimarisini yeniden tanımlayan tarihsel bir kırılmadır.

Bu dönüşüm devletin rolünü de değiştirmektedir. Uzun yıllar boyunca devletlerin temel görevi piyasaları düzenlemek olarak görülürken, bugün devletlerin aynı zamanda dijital altyapıları yöneten, kritik teknolojileri destekleyen ve veri ekosistemlerini şekillendiren aktörler haline geldiği görülmektedir. ABD'nin yarı iletken ihracat kontrolleri, Çin'in devlet kontrollü dijital ekosistemi ve Avrupa Birliği'nin düzenleme gücü üzerinden kurduğu dijital yönetim modeli, teknolojinin artık doğrudan jeopolitik rekabetin temel araçlarından biri olduğunu göstermektedir. Bu nedenle dijital politika, sanayi politikası, dış politika ve ulusal güvenlik politikası arasındaki sınırlar giderek ortadan kalkmaktadır.

Bu çalışmada incelenen örnekler aynı zamanda önemli bir gerçeğı ortaya koymaktadır: Dijital egemenlik yalnızca teknoloji üretme kapasitesine sahip olmakla sağlanamamaktadır. Teknolojiyi geliştirmek kadar onu yöneten hukuki çerçeveyi oluşturmak, standartları belirlemek, veri akışlarını yönetmek ve kurumsal kapasiteyi inşa etmek de egemenliğin ayrılmaz parçalarıdır. Avrupa Birliği'nin Brüksel Etkisi, bunun en açık örneğidir. Küresel ölçekte en büyük dijital platformlara sahip olmamasına rağmen Avrupa Birliği, geliştirdiğı düzenlemeler aracılığıyla küresel teknoloji şirketlerinin davranışlarını şekillendirebilmektedir [29]. Bu durum, norm koyabilmenin de en az teknoloji geliştirebilmek kadar stratejik bir güç unsuru olduğunu göstermektedir.

Bununla birlikte çalışmanın ulaştığı önemli sonuçlardan biri de dijital egemenliğin mutlak bir bağımsızlık projesi olmadığıdır. Günümüz dijital ekonomisinde hiçbir ülkenin tüm teknoloji katmanlarında kendi kendine yeterli hale gelmesi gerçekçi görünmemektedir. Yarı iletken üretiminden büyük dil modellerine, bulut altyapılarından telekom ekipmanlarına kadar uzanan değer zinciri küresel ölçekte dağılmış durumdadır. Dolayısıyla dijital egemenlik, bütün bağımlılıkları ortadan kaldırmak değil; hangi bağımlılıkların kabul edilebilir, hangilerinin ise stratejik risk oluşturduğunu ayırt edebilme kapasitesidir. Başka bir ifadeyle mesele, bağımlılığı sıfırlamak değil; bağımlılığı yönetilebilir hale getirmektir.

Bu perspektif Türkiye açısından özel önem taşımaktadır. Türkiye'nin mevcut dijital dönüşümü büyük ölçüde küresel platformların altyapıları üzerinde gerçekleşmektedir. Arama motorlarından mobil işletim sistemlerine, bulut bilişimden dijital reklamcılığa kadar birçok kritik katmanda yabancı teknoloji şirketlerine yüksek düzeyde bağımlılık bulunmaktadır. Bununla birlikte son yıllarda Siber Güvenlik Kanunu, Yerli İkame Zorunluluğı, Ulusal Yapay Zekâ Stratejisi ve yapay zekâ alanındaki yeni kurumsal girişimler, bu bağımlılıkların artık kamu politikası gündemine girdiğini göstermektedir. Asıl mesele ise bu farkındalığın kalıcı kurumsal kapasiteye dönüşüp dönüşmeyeceğidir.

Bu noktada Türkiye'nin önünde, dijital ekonominin kuralları başkaları tarafından belirlenirken yalnızca bu kurallara uyum sağlamaya çalışan bir ülke olmak ile uluslararası standartların oluşum sürecine katkı sunan bir ülke olmak şeklinde bir yol ayrımı vardır. Türkiye'nin orta ve uzun vadeli hedefi yalnızca dijital teknolojileri kullanan değil; aynı zamanda bu teknolojilerin hukuki, etik ve ekonomik çerçevesini şekillendiren ülkeler arasında yer almak olmalıdır.

Nitekim bu çalışmanın tamamlanma sürecinde, 18 Ağustos 2026 tarihli Resmî Gazete'de yayımlanan Türkiye Yapay Zekâ Eylem Planı (2026-2030), bu raporda savunulan bütüncül dijital egemenlik yaklaşımıyla önemli ölçüde örtüşen bir politika çerçevesi ortaya koymuştur. "Fark Et, İstifade Et, Üret ve Yönet" eksenleri etrafında; insan kaynağı, veri altyapısı, hesaplama kapasitesi, yerli model geliştirme ve yönetişimi tek bir yol haritasında bütünləştiren Plan; dijital egemenliğin ancak rekabet hukuku, veri koruma, siber güvenlik ve yapay zekâ politikalarının ortak bir vizyon altında ele alınmasıyla sağlanabileceği yönündeki temel tezimizi teyit etmektedir. Planın, tüm eylemleri hedef-bütçe-zaman uyumu, durum göstergeleri ve bağımsız değerlendirme bileşeni üzerinden kamuya açık biçimde izleyecek bir Ulusal Yapay Zekâ İlerleme ve Şeffaflık Portali öngörmesi; bu çalışmada tekrar tekrar vurgulanan farkındalığın kalıcı kurumsal kapasiteye dönüşmesi meselesi açısından umut verici bir yaklaşımdır. Nihai olarak Plan'ın tanımladığı hedeflerin somut ve sürdürülebilir kurumsal kapasiteye dönüştürülmesi, tutarlı finansman mekanizmalarıyla desteklenmesi ve enerjiden düzenlemeye uzanan tamamlayıcı politikalarla eşgüdüm içinde yürütülmesi; Türkiye'nin dijital egemenlik yolculuğunda belirleyici olacaktır. Böylece dijital egemenlik, yalnızca savunulan değil; aynı zamanda üretilen ve şekillendirilen bir kapasiteye dönüşme imkânı bulacaktır.

Bu hedefe ulaşabilmek için kamu kurumlarının teknik kapasitesinin güçlendirilmesi, kritik dijital altyapıların sistematik biçimde haritalandırılması, veri yönetişimi mekanizmalarının geliştirilmesi ve rekabet hukuku araçlarının dijital ekonominin gerçeklerine uyarlanması büyük önem taşımaktadır. Aynı zamanda yapay zekâ alanında yerli hesaplama altyapısının geliştirilmesi, Türkçe büyük dil modellerinin desteklenmesi ve kamu verisinin güvenli biçimde inovasyon ekosistemine kazandırılması, yalnızca teknolojik gelişme açısından değil; uzun vadeli stratejik özerklik bakımından da kritik öneme sahiptir.

Bunun yanında dijital egemenlik yalnızca devlet merkezli bir mesele olarak da değerlendirilmemelidir. Üniversiteler, araştırma merkezleri, özel sektör, girişimcilik ekosistemi ve sivil toplum kuruluşları bu sürecin ayrılmaz bileşenleridir. Nitelikli insan kaynağı yetiştiremeyen, temel araştırmayı desteklemeyen ve yenilikçi girişimlerin ölçeklenmesine uygun bir ortam oluşturmamayan ülkelerin dijital egemenlik hedeflerine ulaşması mümkün değildir. Bu nedenle dijital egemenlik stratejisi; eğitim, bilim politikası, sanayi politikası ve teknoloji politikası arasında güçlü bir eşgüdüm gerektirmektedir.

Önümüzdeki dönemde yapay zekânın hızla gelişmesiyle birlikte dijital egemenlik tartışmaları yeni bir aşamaya geçecektir. Büyük dil modelleri yalnızca bilgiye erişim araçları olmaktan çıkmakta; karar destek sistemleri, kamu yönetimi uygulamaları, eğitim süreçleri ve ekonomik faaliyetlerin temel bileşenleri haline gelmektedir. Hesaplama kapasitesi, veri

kaynakları ve temel modeller üzerinde yoğunlaşan güç, geleceğin ekonomik ve siyasi rekabetini belirleyecektir. Bu nedenle yapay zekâ çağında egemenlik tartışmaları, veri ve algoritmalar üzerinden yeniden tanımlanacaktır.

Bu çalışma, dijital hegemonyanın yalnızca teknoloji şirketlerinin büyüklüğüyle açıklanamayacağını; ekonomik yoğunlaşma, hukuki yetki genişlemesi, devlet-teknoloji bütünleşmesi, veri egemenliği ve algoritmik yönlendirme kapasitesinin birlikte oluşturduğu çok katmanlı bir güç mimarisi olduğunu ortaya koymaktadır. Bu mimari karşısında geliştirilecek politikaların da aynı ölçüde bütüncül olması gerekmektedir. Rekabet hukuku tek başına yeterli değildir; veri koruma hukuku tek başına yeterli değildir; siber güvenlik ya da yapay zekâ politikaları da tek başına yeterli değildir. Başarı, bu alanları ortak bir dijital egemenlik vizyonu altında bütünleştirebilen ülkelerin olacaktır.

Sonuç olarak dijital egemenlik, 21. yüzyılın en temel kamu politikası meselelerinden biridir. Egemenlik artık yalnızca sınırların korunması değil; verinin korunması, algoritmaların denetlenmesi, kritik altyapıların yönetilmesi ve teknolojik bağımlılıkların stratejik biçimde yönetilebilmesidir. Dijital çağın egemen devletleri, en fazla teknoloji satın alan devletler değil; teknolojiyi yöneten, düzenleyen, denetleyen ve gerektiğinde alternatiflerini üretebilen devletler olacaktır. Türkiye'nin önünde duran temel soru da budur: Dijital dönüşümün pasif bir tüketicisi mi olacak, yoksa dijital geleceğin kurallarını şekillendiren ülkeler arasında yer alabilecek mi? Bu soruya verilecek cevap, salt teknoloji politikasını teşkil etmenin ötesinde; Türkiye'nin uzun vadeli ekonomik rekabet gücünü, ulusal güvenliğini ve uluslararası sistem içindeki stratejik konumunu da belirleyecektir.

KAYNAKA

- [1] Couture, S., & Toupin, S. (2019). What Does the Notion of “Sovereignty” Mean When Referring to the Digital? *New Media & Society*, 21(10), 2305–2322.
- [2] United Nations Conference on Trade and Development (UNCTAD). (2021). *Digital Economy Report 2021*. UNCTAD.
- [3] Pohle, J., & Thiel, T. (2020). Digital Sovereignty. *Internet Policy Review*, 9(4).
- [4] United States Congress. (2018). *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*.
- [5] Musoni, M., Karkare, P., Teevan, C., & Domingo, E. (2023). Global Approaches to Digital Sovereignty: Competing Definitions and Contrasting Policy. ECDPM Discussion Paper
- [6] Gramsci, A. (1971). *Selections from the Prison Notebooks*. International Publishers.
- [7] Srnicek, N. (2017). *Platform Capitalism*. Polity Press.
- [8] Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- [9] Katz, M. L., & Shapiro, C. (1985). Network Externalities, Competition, and Compatibility. *American Economic Review*, 75(3), 424–440.
- [10] Farrell, J., & Klemperer, P. (2007). Coordination and Lock-In: Competition with Switching Costs and Network Effects. In *Handbook of Industrial Organization* (Vol. 3). Elsevier.
- [11] European Union. (2022). *Regulation (EU) 2022/1925 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)*.
- [12] Synergy Research Group. (2024). *Cloud Market Share Statistics*.
- [13] Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press.
- [14] United States Department of Justice v. Google LLC, Case No. 1:20-cv-03010 (D.D.C.).
- [15] European Commission. (2018). Case AT.40099 – Google Android.
- [16] Cr  mer, J., de Montjoye, Y.-A., & Schweitzer, H. (2019). *Competition Policy for the Digital Era*. European Commission Report.
- [17] United States v. Google LLC, Case No. 1:23-cv-00108-LMB-JFA (E.D. Virginia).
- [18] Harris, S. (2024). The Rise of Palantir and the Militarization of Big Data. *Foreign Policy*.
- [19] U.S. Department of Defense. (2022). *Joint Warfighting Cloud Capability (JWCC) Contract Award*. DoD Press Release. <https://www.defense.gov/News/Contracts/Contract/Article/3212589/>
- [20] Amazon Web Services. (2022). AWS Secret and Top Secret Regions for Intelligence Community. *AWS Public Sector Blog*. <https://aws.amazon.com/blogs/publicsector/aws-secret-region/>
- [21] Wakabayashi, D., & Shane, S. (2018). Google Will Not Renew Pentagon Contract That Upset Employees. *The New York Times*.
- [22] Sakelaris, N. (2025). Palantir, Anduril Reportedly Building Tech Consortium to Bid on Pentagon Contracts. *Yahoo Finance*. <https://finance.yahoo.com/news/palantir-anduril-reportedly-building-tech-221208996.html>
- [23] Yahoo Finance Markets. (2025). Palantir Stock Jumps on Defense Tech Partnerships Including Performance Drone Works, Ondas, and World View. *Yahoo Finance*. <https://finance.yahoo.com/markets/stocks/articles/palantir-stock-jumps-defense-tech-133951017.html>

- [24] ENISA – European Union Agency for Cybersecurity. (2023). *Threat Landscape Report*.
- [25] European Parliament Research Service. (2022). *Digital Sovereignty for Europe: From Vision to Capacity*.
- [26] U.S. Department of Commerce, Bureau of Industry and Security. (2023). Export Controls on Advanced Computing and Semiconductors to China. *Federal Register*.; The White House. (2025). Executive Order 14179 on Removing Barriers to American Leadership in Artificial Intelligence.
- [27] People's Republic of China. (2017). *National Intelligence Law of the People's Republic of China*. Standing Committee of the National People's Congress.
- [28] Kania, E. B. (2019). *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*. Center for a New American Security.
- [29] Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.
- [30] Court of Justice of the European Union. (2020). *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II)*, Case C-311/18.
- [31] Kissinger, H., Schmidt, E., & Huttenlocher, D. (2021). *The Age of AI: And Our Human Future*. Little, Brown and Company.
- [32] Allen, G. C. (2025). DeepSeek, Huawei, Export Controls, and the Future of the U.S.-China AI Race. Center for Strategic and International Studies (CSIS).
- [33] Bommasani, R. et al. (2021). *On the Opportunities and Risks of Foundation Models*. Stanford University.
- [34] European Union. (2024). *Artificial Intelligence Act (AI Act)*.
- [35] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2021). *Ulusal Yapay Zekâ Stratejisi 2021-2025*. Cumhurbaşkanlığı Genelgesi, Resmî Gazete.
- [36] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2024). *Ulusal Yapay Zekâ Stratejisi 2024-2025 Eylem Planı*.
- [37] N Partners Hukuk Bürosu. (2025). Türkiye'de 2026 Yapay Zekâ Kanunu: TBMM'ye Sunulan Üç Kanun Teklifinin Detaylı Karşılaştırılması. <https://npartners.com.tr/tr/turkiye-de-2026-yapay-zeka-kanunu-tbmm-ye-sunulan-uc-kanun-teklifinin-detayli-karsilastirilmesi>
- [38] Van Dijck, J., Poell, T., & de Waal, M. (2018). *The Platform Society: Public Values in a Connected World*. Oxford University Press.
- [39] Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.
- [40] Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51(8), 56–59.
- [41] Sunstein, C. R. (2017). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.
- [42] European Union. (2022). *Regulation (EU) 2022/2065 (Digital Services Act – DSA)*.
- [43] Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

- [44] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2023). *Kamu Bulut Bilişim Stratejisi ve Eylem Planı Taslağı*. <https://cbddo.gov.tr/proje-aciklamasi/6597/bulut-bilisim-stratejisi/>
- [45] IAB Türkiye. (2023). *Dijital Reklam Yatırımları Raporu*. İnteraktif Reklamcılık Derneği.
- [46] Reklamcılar Derneği, IAB Türkiye & Deloitte. (2025). *Türkiye’de Tahmini Medya ve Reklam Yatırımları 2024 Raporu*. Nisan 2025. https://iabtr.org/wp-content/uploads/2025/04/Medya-ve-Reklam-Yatirimlari-2024_compressed-1.pdf
- [47] Ulusal Siber Olaylara Müdahale Merkezi (USOM). (2024). *2024 Yılı Siber Tehdit Durum Raporu*. Bilgi Teknolojileri ve İletişim Kurumu.
- [48] Türkiye Cumhuriyeti. (2025). **7545 sayılı Siber Güvenlik Kanunu**. 19 Mart 2025 tarihli Resmî Gazete.
- [49] CyberArts. (2025). Siber Bülten 2025: Kritik Altyapı Güvenliğinde Milli Teknoloji Hamlesi. <https://www.cyberartspro.com/tr/cyberarts-siber-bulten-2025/>
- [50] We Are Social & Meltwater. (2025). *Dijital 2025 Türkiye Raporu*. <https://datareportal.com/reports/digital-2025-turkey>
- [51] HaberTürk. (2025). Türkiye’nin Teknoloji Devleri Yabancı Ellerde: E-Ticaret ve Girişim Ekosistemi Küresel Sermayeye Teslim mi Oluyor? <https://www.haberturk.com/turkiye-nin-teknoloji-devleri-yabanci-ellerde-3788903-teknoloji>
- [52] Wu, T. (2018). *The Curse of Bigness: Antitrust in the New Gilded Age*. Columbia Global Reports.
- [53] Khan, L. M. (2017). Amazon’s Antitrust Paradox. *Yale Law Journal*, 126(3), 710–805.
- [54] Autorité de la concurrence & Bundeskartellamt. (2016). *Competition Law and Data*.
- [55] Rekabet Kurumu. (2023). *Dijital Dönüşümün Rekabet Hukukuna Yansımaları*. I. Denetim ve Uygulama Dairesi. <https://www.rekabet.gov.tr/Dosya/dijital-piyasalar-calisma-metni.pdf>
- [56] Türkiye Cumhuriyeti. (2016). **6698 sayılı Kişisel Verilerin Korunması Kanunu**.
- [57] Graef, I. (2016). *EU Competition Law, Data Protection and Online Platforms*. Kluwer Law International.
- [58] Celeste, E. (2019). Digital Constitutionalism: A New Systematic Theorisation. *International Review of Law, Computers & Technology*, 33(1), 76–99.
- [59] Türk Telekom & Huawei. (2025). Türk Telekom ve Huawei’den Akıllı Şehircilik Alanında Avrupa’da Bir İlk. *Türk Telekom Medya Merkezi*. <https://medya.turktelekom.com.tr/turk-telekom-ve-huawei-den-akilli-sehircilik-alaninda-avrupa-da-bir-ilk>
- [60] Euronews Türkçe. (2025). AWS Çöküşü: Bulut Bilişim Sistemi Neden Değişmeli? <https://tr.euronews.com/next/2025/10/22/aws-cokusu-bulut-bilisim-sistemi-neden-degismeli>
- [61] Haberler.com. (2026). Türkiye’nin İlk Yerli Uç Nokta Güvenlik Platformu Milli Savunma Bakanlığı’na Teslim Edildi. <https://www.haberler.com/guncel/turkiye-nin-ilk-yerli-u-c-nokta-guvenlik-platformu-teslim-edildi-19856844-haberi/>
- [62] Gartner. (2023). *Sovereign Cloud Strategy and Architecture Trends*.
- [63] OECD. (2024). *OECD Digital Economy Outlook*.
- [64] European Commission. (2020). *Shaping Europe’s Digital Future*.
- [65] Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*.

- [66] European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)*.
- [67] European Union Agency for Fundamental Rights (FRA). (2020). *Getting the Future Right: Artificial Intelligence and Fundamental Rights*.
- [68] Court of Justice of the European Union. (2014). *Google Spain SL v AEPD and Mario Costeja González*, Case C-131/12.
- [69] Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112.
- [70] IMF. (2024). *Gen-AI: Artificial Intelligence and the Future of Work*.
- [71] European Data Protection Board (EDPB). (2023). *Guidelines on Generative AI and Personal Data*.
- [72] UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*.
- [73] NIST – National Institute of Standards and Technology. (2023). *AI Risk Management Framework*.
- [74] Roberts, H., Cows, J., Morley, J., et al. (2021). The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation. *AI & Society*.
- [75] Acemoğlu, D., & Johnson, S. (2023). *Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity*. PublicAffairs.
- [76] Helberger, N., Pierson, J., & Poell, T. (2018). Governing Online Platforms: From Contested to Cooperative Responsibility. *The Information Society*, 34(1), 1–14.
- [77] Gaia-X Project Documentation and Policy Papers.
- [78] World Bank. (2021). *World Development Report 2021: Data for Better Lives*.
- [79] Türkiye Cumhuriyeti Gelir İdaresi Başkanlığı. (2020). 7194 **sayılı** Dijital Hizmet Vergisi ile Bazı Kanunlarda ve 375 sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun. Resmî Gazete, 7 Aralık 2019.
- [80] OECD. (2023). *Tax Challenges Arising from the Digitalisation of the Economy – Global Anti-Base Erosion Model Rules (Pillar Two)*. OECD/G20 Inclusive Framework on BEPS. <https://www.oecd.org/tax/beps/global-anti-base-erosion-model-rules-pillar-two.htm>
- [81] European Commission. (2023). *Data Act*.
- [82] European Commission. (2022). *Data Governance Act*.
- [83] DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.
- [84] European Commission. (2021). *Europe's Digital Decade: Digital Targets for 2030*.

YAZARLAR HAKKINDA

İmran Gürakan

İmran Gürakan, Orta Doğu Teknik Üniversitesi İstatistik Bölümü mezunu olup Hacettepe Üniversitesi'nde İşletme alanında yüksek lisansını tamamlamıştır. Güney Kore ve Amerika'da girişimcilik ve teknoloji politikaları üzerine çeşitli eğitim programlarına katılmıştır. Teknoloji, girişimcilik, yatırım ve kamu politikaları alanlarında 14 yılı aşkın deneyime sahiptir. Ankara TEKMER ve LEAP Investment'ın Kurucu Ortağı ve Genel Müdürü olan Gürakan, teknoloji girişimi yatırımcısı olarak girişimlerin ölçeklenmesi üzerine çalışmalar yürütmekte; özellikle yapay zekâ, siber güvenlik, savunma ve çift kullanımlı teknolojilere odaklanmaktadır. Yatırım yaptığı bazı girişimlerin yönetim kurullarında görev alarak stratejik büyüme ve ölçeklenme süreçlerine de katkı sağlamaktadır. T.C. Sanayi ve Teknoloji Bakanlığı Teknogirişim Konseyi'nin 30 üyesinden biri olan Gürakan, Türkiye'de savunma alanının gelişimine yönelik çeşitli strateji ve çalışma komitelerinde de görev almaktadır. Ayrıca uluslararası platformlarda bağımsız değerlendirici olarak ileri teknoloji ve çift kullanımlı girişimlerin değerlendirilmesine katkı sağlamaktadır.

Çiğdem Gizem Okkaoğlu

Çiğdem Gizem Okkaoğlu, 2015 yılında Bilkent Üniversitesi Endüstri Mühendisliği Bölümü'nden mezun oldu. Rekabet Kurumunda beş yıl çalıştı, ardından Balcıoğlu Selçuk Ardiyok Keki Avukatlık Ortaklığı'nda (Dentons Türkiye) Danışman, ELİG Gürkaynak Avukatlık Bürosu'nda Kıdemli Avukat, Günay Erdoğan Avukatlık Bürosu'nda Ortak Avukat olarak çalıştı. Okkaoğlu, ayrıca Ankara Üniversitesi Hukuk Fakültesi'nden 2019; Anadolu Üniversitesi İktisat Bölümü'nden 2018 ve Sosyal Hizmetler Bölümü'nden 2012 yılında mezun oldu. Yüksek lisansını Orta Doğu Teknik Üniversitesi Avrupa Çalışmaları Tezli Yüksek Lisans Programında tamamladı. Halihazırda teknoloji hukuku ve teknoloji politikası alanında çalışmalar yürütmekte ve hukuk danışmanı olarak çalışmaktadır.



Cevizlidere Mah. Mevlana Bulv. No:123/305 Çankaya/Ankara
0312 939 93 00 | info@toplum.org.tr | www.toplum.org.tr